CORRECTIONS AND REENTRY:

Protected Health Information Privacy Framework for Information Sharing

Corrections and Reentry:
Protected Health Information Privacy Framework for Information Sharing

Executive Summary

BARRIERS TO JUSTICE/HEALTH INFORMATION EXCHANGES

Nationwide polls show that Americans continue to be deeply concerned about the privacy and security of their protected health information (PHI), particularly when it is in electronic form, illustrating an ongoing challenge of balancing society's need to improve the quality, safety, and efficiency of health care with the protection of PHI.[1] The field of corrections, which includes incarceration, pretrial, probation, and parole, is no different. During the correctional process, an individual may receive medical, mental health, and/or substance abuse testing, assessment and/or treatment and, upon release, be referred for follow-up treatment in the community. Successful rehabilitation of these individuals and their ability to reintegrate into society upon release depends, to a large degree, upon the beneficial communication about their needs, treatment matching, and continuity of care.

Legal and technical barriers, both real and perceived, often prevent a smooth exchange of PHI among justice-to-health systems (and vice versa) and impede appropriate diagnosis, treatment, diversion, and transition of individuals while they are involved in the criminal justice system. For example, community treatment providers still cite confidentiality and the Health Insurance Portability and Accountability Act (HIPAA) as the primary reasons why they cannot or will not share PHI. However, HIPAA's restrictions on sharing PHI are often misunderstood, which has resulted in practitioners' misapplying the law to be far more restrictive than the actual regulatory language requires.[2] In many cases, the fear associated with these laws is inflated, and a careful examination, with corresponding changes in practice (e.g., obtaining consent forms), can alleviate most concerns. Other common concerns include an absence of rapport between agencies and limited knowledge of each other's capabilities.[3]

A gap exists in the public health and public safety paradigms. The two are interrelated, with drug abusers three to four times more likely to commit a crime and individuals with a mental illness two to three times more likely to be incarcerated. Yet limited communication exists between justice and health agencies.[4] Recidivism is high. It makes up a large proportion of the admittances to prisons or jails (in some jurisdictions, more than half of all incoming individuals). As many as 40 percent of adult prisoners are likely to recidivate (i.e., commit a new crime or get revoked on a technical violation) within three years of release.[5] Further, many individuals released to the community possess a history of substance abuse and/or mental illness as well as other medical disorders and ailments which, if left untreated, impede their ability to find employment and demonstrate prosocial behaviors.[6]

MAKING THE CASE FOR A PHI PRIVACY FRAMEWORK

For successful reentry, the exchange of PHI for diagnosis, treatment, and continuity of care is critical. Approximately 10 million people spend time in correctional facilities at some point each year. They are more likely than those in the general population to have behavioral health problems (i.e., mental health problems and addictions), communicable diseases (e.g., tuberculosis, Hepatitis C, and HIV infection), and chronic illnesses (e.g., diabetes, asthma, and hypertension).[7,8] This population is often at its sickest when detained, frequently experiencing a psychiatric crisis and/or active addiction.[9] In fact, 85 percent of jail detainees and 65 percent of prisoners (seven times the rate of the general population) are believed to be substance-involved.[10] Despite these stark findings, less than 20 percent of inmates will receive any formal treatment for their addictions while incarcerated.[11] According to the Bureau of Justice Statistics (BJS), in mid-year 2005 nearly half of all inmates (federal, state, and local) reported having some mental health problem.[12] These individuals are often the poorest, often homeless, and the most severely challenged in all aspects of community life.

While the Patient and Affordable Care Act (ACA), which was signed into law in March 2010,[13] may potentially aid individuals who are at risk for incarceration and those who have been incarcerated through new eligibility for Medicaid, it will also further illuminate the barriers between corrections and the health community to share PHI. This increased use of medical, behavioral, and substance abuse services is another reason why the exchange of PHI between corrections and providers is so crucial. Pretrial, probation, and parole agencies, as well as jails and prisons, are in a position to identify individuals who are newly eligible for Medicaid. Involving these entities in designing processes for enrolling individuals and for connecting them with community-based care upon release is important for improving the continuity of care between community- and corrections-based care and, in turn, maximizing the investment local and state governments make in correctional health care.[14]

Reentry into the community is a vulnerable time, marked by difficulties in adjusting, increased drug use, and a 12-fold increased risk of death in the first two weeks after release.[15] Effective transition planning and implementation can minimize the risk of these hazards; enhance public safety by increasing the possibility that individuals will participate in, and complete, supervision and treatment requirements; and improve individual outcomes. If effective PHI sharing occurs at—or ideally, prior to—an individual's release to the community, it may result in:

- Improved continuity of care.
- Improved individual physical and behavioral health.
- Improved public safety.
- Enhancement of criminal justice and other agencies' ability to implement evidence-based practices.
- Long-term reductions in costs associated with reductions in recidivism.
- The support of efforts to translate the research/literature on "what works" with individuals involved with the criminal justice system into more efficacious policies and practices (which may reduce the likelihood of recidivism and promote community safety).[16]

In order for corrections entities to effectively address the issues highlighted here and ensure compliance with HIPAA (for medical and mental health information), as well as with Title 42: Public Health, Part 2—Confidentiality of Substance Abuse Patient Records (42 CFR Part 2, for substance abuse information), a privacy framework must be established and implemented. A privacy framework involves not only the correctional entity and its commitment to adhere to laws and protect PHI, but also includes authorization to share PHI by the individual and—when appropriate—the courts. Also essential is the development of relationships and agreements between correctional entities and outside organizations that perform functions or services for the entity.

In sum, a privacy framework comprises three components:

1. A privacy policy to articulate the entity's position to protect medical, mental health, and substance abuse diagnosis and treatment information—or PHI; adhere to legal requirements; and specify the rules and procedures for such compliance. A well-developed and implemented PHI privacy policy protects the entity, the individual, and the public and contributes to reduced recidivism by establishing a mechanism for continuity of care and treatment.

2. Individual consent authorizations and/or court orders authorizing the sharing of PHI between corrections and community treatment providers. Obtaining permission from an individual to release his or her PHI is a straightforward way to facilitate information sharing.

3. Contractual agreements between correctional entities and outside organizations that perform a specified set of functions or provide services to or on behalf of the entity. Such agreements define the parameters of PHI disclosure and specifically articulate what the organization has been engaged to do. They require assurances that the organization will comply with PHI privacy and security regulations.

The PHI maintained by entities—if handled inappropriately—can cause problems for those affected. In worst cases, personal and public safety may be jeopardized. These issues affect the whole justice community, including law enforcement, prosecution, defense, courts, pretrial, parole, probation, corrections, and victim services, as well as members of the public. A well-developed and implemented PHI privacy framework protects the individual and the entity and enables the appropriate handling of this critical information.

RESOURCE OVERVIEW

The *Corrections and Reentry: Protected Health Information Privacy Framework for Information Sharing* PHI Framework Guide was developed by the Institute for Intergovernmental Research with funding support from the American Probation and Parole Association (APPA) and the Association of State Correctional Administrators (ASCA) under cooperative agreements by the Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), U.S. Department of Justice (DOJ). The purpose of the framework guide is to provide recommendations for addressing the issues described earlier in this brief: the protection, handling, and exchange of PHI between corrections and health providers in compliance with federal law.

This resource was designed to enable correctional entities to comply with HIPAA and 42 CFR Part 2 in the receipt or sharing of PHI, whether the correctional entity meets HIPAA's designation of a "covered entity,"[17] is determined by 42 CFR Part 2 to be a "federally assisted program,"[18] or does not meet either criteria. The tools within the resource may

be used by any correctional entity interested in articulating its commitment to protecting PHI and implementing the components of a privacy framework.

The PHI Framework Guide features an in-depth overview of HIPAA and 42 CFR Part 2 and describes how the regulations may apply to the entity. PHI policy provisions, contained in the policy development template chapter, are provided to assist entities in developing PHI privacy policies related to the medical, mental health, and, if applicable, substance abuse testing and treatment information the entities collect, receive, maintain, archive, access, and disclose to entity personnel; other correctional entities; participating criminal justice and public safety agencies; as well as to community medical, mental health, and substance abuse treatment providers. Each policy section comprises a fundamental component of a comprehensive PHI privacy policy that includes baseline provisions on information collection, information quality, collation and analysis, merging of records, information access and disclosure, redress, security safeguards, retention and destruction, accountability and enforcement, and training.

Template policy provisions are grouped according to related policy concepts and are presented in a user-friendly question-and-answer format to enable policy authors, prompted by key policy questions, to draft policy language that answers or addresses each question posed. Where applicable, HIPAA and 42 CFR Part 2 regulations are cited to illustrate how the provision ensures compliance. Sample language is also provided and follows each policy provision to help authors understand the meaning of the question asked and to illustrate how to write policy language that addresses the policy question (e.g., formulate privacy policies).

To further support a PHI privacy framework, this document includes useful tools, such as a sample consent authorization form and a sample contractual agreement, each of which meets both HIPAA and 42 CFR Part 2 requirements. Additionally, a PHI Policy Review Checklist is provided as a tool to enable entities to evaluate pre-established PHI policies to ensure that they are in compliance with the law or to use when performing an annual PHI policy review. Other resources include a sample court order, a confidentiality notice, a glossary of terms and definitions, a listing of applicable federal PHI privacy laws, and a resource list.

WHY USE THIS RESOURCE

Receipt and sharing of protected health information is critical for individuals entering or leaving the corrections environment. Establishing and implementing a PHI privacy framework among corrections entities and medical, behavioral, and substance abuse treatment providers using this resource will strengthen trust and public confidence by promoting effective and responsible sharing of PHI that supports fundamental privacy concepts. A comprehensive PHI privacy framework—composed of a well-developed privacy policy, documented and implemented individual consent authorizations, and compliant contractual agreements—is the fundamental linchpin to a system of trust that justice agencies are serving as responsible stewards of PHI. Implementing such a framework further supports the mission of corrections to protect public safety; enables the provision of proper care for offenders; and improves the transition of released individuals into society.

Endnotes

[1] *Making it Meaningful: How Consumers Value and Trust Health IT*, National Partnership for Women and Families, Washington, February 2012, www.nationalpartnership.org/site/PageServer?pagename=issues_health_IT_survey.
[2] *Information Sharing in Criminal Justice—Mental Health Collaborations: Working with HIPAA and Other Privacy Laws*, Petrila, John, J.D., L.L.M, and Fader-Towe, Hallie, J.D., Justice Center, The Council of State Governments, supported by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, 2010.
[3] *Justice-Health Collaboration: Improving Information Exchange Between Corrections and Health/Human Services Organizations*, Making the Case for Improved Reentry and Epidemiological Criminology, Matz, A. K., Wicklund, C., Douglas, J., and May, B., jointly developed by the American Probation and Parole Association, SEARCH, and the Association of State Correctional Administrators, September 2012; see also Matz, A. K. (2013). Leveraging technology to enhance corrections-health and human service information sharing and offender reentry. In E. Waltermaurer and T. Akers (eds.), *Epidemiological criminology: Theory to practice* (pp. 187–196). New York: Routledge.
[4] *Ibid*.
[5] *State of Recidivism: The Revolving Door of America's Prisons*, Pew Center on the States (2011), Pew Charitable Trusts, Washington, DC.
[6] *Justice-Health Collaboration: Improving Information Exchange Between Corrections and Health/Human Services Organizations*, Making the Case for Improved Reentry and Epidemiological Criminology, Matz, A. K., Wicklund, C.,

Douglas, J., and May, B., jointly developed by the American Probation and Parole Association, SEARCH, and the Association of State Correctional Administrators, September 2012; see also Matz, A. K. (2013).

[7] *Medical Problems of Jail Inmates* (NCJ 210696), Maruschak, L. M., Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, Washington, DC, 2006.

[8] *Mental Health Problems of Prison and Jail Inmates* (NCJ 213600), James, D. J. and Glaze, L. E., Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, Washington, DC, 2006.

[9] *Health Information Privacy in the Correctional Environment*, issue paper, Goldstein, Melissa M., J.D., George Washington University, Community Oriented Correctional Health Services, April 2012.

[10] *Behind Bars II: Substance Abuse and America's Prison Population,* National Center on Addiction and Substance Abuse, New York, 2010.

[11] *Increasing effective communication between criminal justice and treatment settings using health information technology* (draft), unpublished report, Treatment Research Institute, 2011.

[12] *Health Information Privacy in the Correctional Environment*, issue paper, Goldstein, Melissa M., J.D., George Washington University, Community Oriented Correctional Health Services, April 2012

[13] Affordable Care Act, U.S. Department of Health and Human Services, http://www.hhs.gov/opa/affordable-care-act/index.html.

[14] *The Affordable Care Act: Implications for Public Safety and Corrections* Populations, Phillips, S. D., The Sentencing Project, www.sentencingprooject.org, September 2012.

[15] *Release from prison—a high risk of death for former inmates,* Binswanger, I. A., Stern, M. F., Deyo, R. A., et al., New England Journal of Medicine, 2007; 356(3):157–65.

[16] *Justice-Health Collaboration: Improving Information Exchange Between Corrections and Health/Human Services Organizations*, Making the Case for Improved Reentry and Epidemiological Criminology, Matz, A. K., Wicklund, C., Douglas, J., and May, B., jointly developed by the American Probation and Parole Association, SEARCH, and the Association of State Correctional Administrators, September 2012; see also Matz, A. K. (2013).

[17] Covered entity—per 45 Code of Federal Regulations, Part 160, General Administrative Requirements, Subpart A, § 160.103 Definitions, is defined as a health plan; a health-care clearinghouse; a health-care provider who transmits any health information in electronic form in connection with a covered transaction [relating to a health claim report, status, payment, etc.].

[18] Federally assisted program—defined in 42 Code of Federal Regulations, Part 2, §§ 290dd-2, 42 CFR 2.11, is defined as a program which includes any individual or entity (other than a general medical care facility) that holds itself out as providing, in whole or in part, substance abuse diagnosis, treatment, referral for treatment or prevention; or an identified unit within a general medical facility which holds itself out as providing, and provides, substance abuse diagnosis, treatment, referral for treatment, or prevention; or medical personnel or other staff in a general medical facility whose primary function is the provision of substance abuse diagnosis, treatment, referral for treatment, or prevention, and who are identified as such providers. See 42 CFR Part 2 Subpart B § 2.12(e)(1) for examples.

Corrections and Reentry: Protected Health Information Privacy Framework for Information Sharing

Christina Abernathy
Senior Research Associate
Institute for Intergovernmental Research (IIR)

American Probation and Parole Association (APPA)
Association of State Correctional Administrators (ASCA)
Institute for Intergovernmental Research (IIR)
Bureau of Justice Assistance (BJA)
Global Justice Information Sharing Initiative (Global)

2014

This project was supported by Grant No. 2009-DD-BX-K138 and 2010-DB-BX-K021 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Where to Locate This Resource

This resource is available online at it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

To Request a Word Version of the Template

To request a Word version, send requests to GLOBAL@iir.com.

About APPA

www.appa-net.org

The American Probation and Parole Association (APPA) is an international association composed of members from the United States, Canada, and other countries actively involved with criminal and juvenile justice in pre-trial, probation, parole, and community-based corrections. All levels of government including local, state/provincial, tribal, and federal agencies are counted among its constituents. By taking the initiative, APPA has grown to become the voice for thousands of pretrial, probation, and parole practitioners including line staff, supervisors, and administrators. APPA provides training and technical assistance, research, information clearinghouse services, and advocacy for its constituents. The association represents a strong, unified voice for the field of community corrections.

About ASCA

www.asca.net

The Association of State Correctional Administrators (ASCA) was founded on the belief that each represented correctional jurisdiction is unique with regard to obligatory statutes, policies, structure, incarcerated population, resources, and burning issues, but that similarities of purpose, responsibilities, principles, and challenges among its member jurisdictions unite them in a quest for public safety, secure and orderly facilities, and professionalism that can be achieved through sharing ideas and vigorously entering into collaborative efforts to continuously improve the corrections profession.

About IIR

www.iir.com

The Institute for Intergovernmental Research (IIR) is a Florida-based nonprofit corporation specializing in criminal justice, homeland security, and juvenile justice issues. IIR has a proven history of promoting greater efficiency and effectiveness among federal, state, local, and tribal criminal justice agencies through customized training, technical assistance, and research. Areas of special competence include criminal justice information sharing, privacy and civil liberties, violence reduction, Gang Resistance Education and Training, anti-gang initiatives, officer safety and wellness, anti-terrorism initiatives, criminal intelligence systems, homicide and narcotics investigations management, and information technology and multimedia development. IIR's standard of excellence, commitment to performance-based solutions, and trusted partnerships are the cornerstone for superior service delivery.

About BJA

www.bja.gov

BJA's mission is to provide leadership and services in grant administration and criminal justice policy development to support local, state, and tribal justice strategies to achieve safer communities. BJA supports programs and initiatives in the areas of law enforcement, justice information sharing, countering terrorism, managing offenders, combating drug crime and abuse, adjudication, advancing tribal justice, crime prevention, protecting vulnerable populations, and capacity building.

About Global

it.ojp.gov/global

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

Please cite this report as (APA):

Abernathy, C. (2014). *Corrections and reentry: Protected health information privacy framework for information sharing.* Lexington, KY: Council of State Governments, American Probation and Parole Association.

Table of Contents

Chapter 1: Introduction

There is an increased emphasis by the criminal justice and corrections systems across the nation to reduce harm and victimization and to make communities safer. This is being accomplished through a number of different initiatives, including offender reentry programs, and an increased emphasis on demonstrating better results focused on the use of research and the implementation of evidence-based practices throughout the criminal justice system processes. Studies examining the question of how best to prevent future crime have important implications for justice system policy and practice. Included in "what works" research are the need to assess risk and to identify effective targets of intervention to reduce future crime; the need to provide appropriate behavior-changing programming; and the need to pair sanctions with interventions that address criminogenic needs. All of this requires better communication and information sharing between criminal justice and correctional agencies and behavioral health treatment providers inclusive of mental health and substance abuse treatment.

I. Protected Health Information and Corrections

The field of corrections is involved in the housing and detention, treatment, rehabilitation, and supervision of persons who have been charged with or convicted of crimes. These functions commonly include incarceration, imprisonment, pre-trial, probation, and parole during which an individual may receive medical, mental health, and/or substance abuse testing and/or treatment. Successful rehabilitation of these individuals and their ability to reintegrate into society upon release depends, to a large degree, on the beneficial communication about their needs, treatment matching, and continuity of care. This communication refers to the exchange of information (receipt and sharing) of an individual's **protected health information** (**PHI**)[1] and collaboration regarding his or her medical, mental health, and/or substance abuse treatment and plan of care.

Receipt and sharing of such information is critical for individuals entering or leaving the corrections environment for purposes of classification, treatment, and continuation of care and include:

- Intake assessments (when an individual enters a correctional facility) to determine the individual's level of risk (to him- or herself, other inmates, and corrections personnel); establishment of a treatment plan and engagement in appropriate treatment programs; updated treatment plans; and engagement in medical, mental health, or substance abuse treatment in the community upon release.

- Informing medical, mental health, or substance abuse treatment providers about a defendant's, probationer's, or parolee's treatment history. Compliance with conditions of pre-trial, probation, or parole, and/or court orders, during which medical, mental health, or substance abuse treatment providers may need to share program completion status and treatment progress with pre-trial, probation, and parole officials and/or courts for reporting purposes.

[1] The Health Insurance and Portability and Accountability Act (HIPAA) uses the term "protected health information," whereas Title 42: Public Health, Part 2—Confidentiality of Substance Abuse Patient Records (42 CFR Part 2) uses the term "patient identifying information." For purposes of this template and ease of reading, the term "protected health information"—or "PHI"—will be used to refer both to PHI and to patient identifying information.

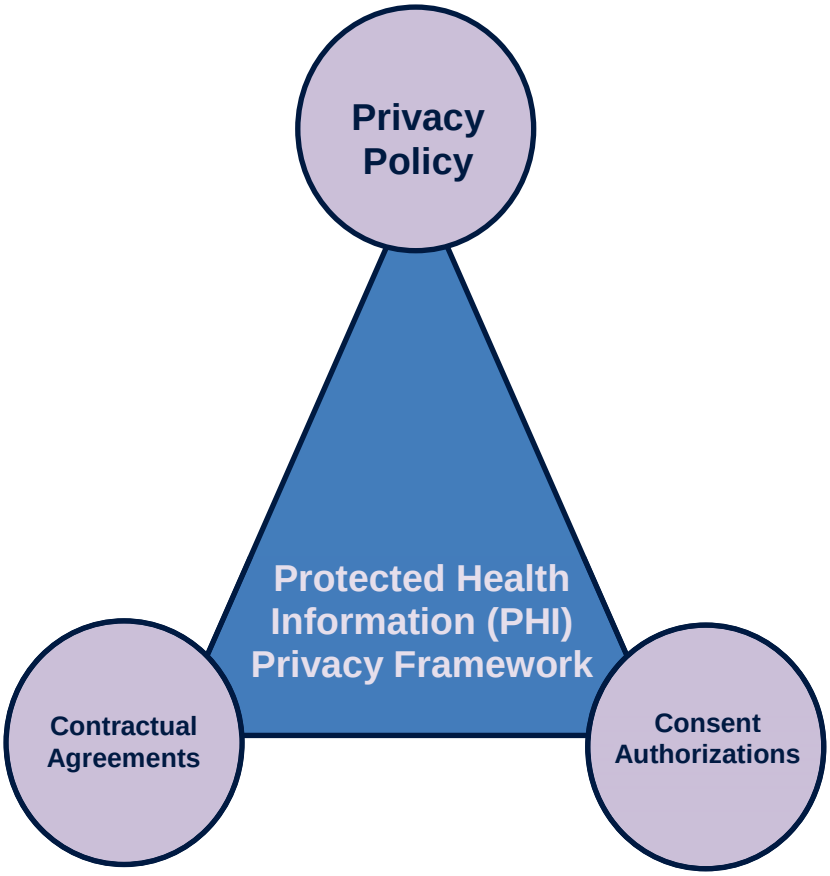
- Reassessment for individuals who reoffend and return to the correctional system (after receiving treatment in the community) for incarceration.

These particular types of information (medical, mental health, and substance abuse information) are governed by federal and state laws that regulate what is permissible to share at the state or local level, primarily through the basic privacy rules for PHI under the Health Insurance Portability and Accountability Act (HIPAA) and substance abuse treatment information covered by Title 42: Public Health, Part 2—Confidentiality of Substance Abuse Patient Records (42 CFR Part 2).[2]

II. PHI Privacy Framework

Medical, mental health, and substance abuse treatment and testing information are considered "protected health information,"[3] each having legal constraints and rules associated with its collection, storage/maintenance, security, access, sharing, retention, and destruction.

Corrections and reentry entities should develop a comprehensive **PHI privacy framework** to ensure that PHI protections are in place for the PHI created, received, and disclosed through the incarceration and release process. This framework is best addressed using a three-component approach, each component established in compliance with the requirements of applicable law: a PHI privacy policy, consent authorizations (and/or court orders), and contractual agreements. This *Corrections and Reentry: Protected Health Information Privacy Framework for Information Sharing* guide contains each of the tools correctional entities need to build such a framework. A PHI Policy Development Template is provided in Chapter 3, and the appendices contain a sample consent authorization form and a sample contractual agreement, each of which meets both HIPAA and 42 CFR Part 2 requirements. Additionally, a PHI Policy Review Checklist is provided as a tool to enable entities to evaluate pre-established PHI policies to ensure that they are in compliance with the law or to use when performing an annual PHI policy review. Other resources include a sample court order, a confidentiality notice, a glossary of terms and definitions, a listing of applicable federal PHI privacy laws, and a resource list.



All three must adhere to HIPAA and 42 CFR Part 2 requirements to ensure a fully compliant PHI framework!

1. PHI Privacy Policy

To address the HIPAA requirement, as well as ensure that the privacy requirements of 42 CFR Part 2 and any particular state-enacted regulations are articulated and implemented, correctional entities **must** establish policies and procedures to comply with these requirements and articulate them in a PHI privacy policy. In simple terms, a PHI privacy policy communicates (within the organization, to external entities that access and share information with the organization, to business associates and other entities, and publicly) that the entity will adhere to the legal requirements and policy and procedural provisions addressing the gathering and sharing of

[2] *Information Sharing in Criminal Justice—Mental Health Collaborations: Working with HIPAA and Other Privacy Laws*, John Petrila, J.D., L.L.M, and Hallie Fader-Towe, J.D., Council of State Governments Justice Center, Bureau of Justice Assistance, Office of Justice Programs, DOJ, www.bja.gov/Publications/CSG_CJMH_Info_Sharing.pdf.

[3] The Health Insurance and Portability and Accountability Act (HIPAA) uses the term "protected health information," whereas Title 42: Public Health, Part 2—Confidentiality of Substance Abuse Patient Records (42 CFR Part 2) uses the term "patient identifying information." **For purposes of this report and ease of reading, the term "protected health information"—or "PHI"—will be used to refer both to PHI and to patient identifying information**.

PHI in a manner that protects constitutional and statutory rights, including personal privacy and other civil liberties and civil rights. A well-developed and implemented PHI privacy policy protects the entity, the individual, and the public and contributes to reduced recidivism by establishing a PHI-sharing framework for purposes of continuity of care and treatment.

HIPAA-covered entities (refer to Chapter 2, section I.A.) must implement—in written or electronic form—policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or other requirements of the privacy rule that define the standards to protect an individual's PHI. Refer to the HIPAA policy requirements below:

- In accordance with 45 CFR Part 164 Subpart C §164.316(a) and (b), a HIPAA-covered entity may change its policies and procedures at any time, provided that the changes are documented and implemented. **Covered entities must maintain the policies and procedures in written (which may be electronic) form**, and will maintain a written (which may be electronic) record of revisions or policy changes (e.g., action, activity, or assessment). Covered entities are required to retain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. The documentation must be made available to those persons responsible for implementing the procedures to which the documentation pertains. Finally, covered entities are required to review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the e-PHI.

- The HIPAA Privacy Rule requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. According to the U.S. Department of Health and Human Services,[4] "the implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. For uses of PHI, the covered entity's policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access."

- In accordance with 45 CFR Part 164 Subpart C § 164.530(i)(2)(i), a covered entity must change its policies and procedures as necessary and appropriate to comply with changes in law, including HIPAA standards, requirements, and implementation specifications.

- In accordance with 45 CFR Part 164 Subpart C § 164.530(i)(3), whenever there is a change in law that necessitates a change to the covered entity's policies and procedures, the entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the [privacy practices] notice required by § 164.520, the entity must promptly make the appropriate revisions to the privacy notice in accordance with § 164.520(b)(3).

Unless effective and compliant PHI privacy policies are being utilized at every level of the entity's PHI-handling operation, the entity may be exposing itself and others to unacceptable risks and penalties from problems caused by failure to honor essential protection expectations. The PHI maintained by entities—if handled inappropriately—can cause problems for those affected. In worst cases, personal and public safety may be jeopardized. These issues affect the whole justice community, including law enforcement, prosecution, defense, courts, pre-trial, parole, probation, corrections, and victim services, as well as members of the public. A well-developed and implemented PHI privacy policy protects the entity and enables the appropriate handing of this critical information.

2. Consent Authorizations

Individual consent authorizations and/or court orders authorize the sharing of PHI between corrections and community treatment providers. Obtaining permission from an individual to release his or her PHI is a straightforward way to facilitate information sharing. A sample HIPAA- and 42 CFR Part 2-compliant consent authorization is contained in Appendix C.

3. Contractual Agreements

HIPAA and, if applicable, 42 CFR Part 2 compliant contractual agreements should be established between correctional entities and outside organizations that perform a specified set of functions or provide services to or on behalf of the entity. Such agreements define the parameters of PHI disclosure and specifically articulate what the organization has been engaged to do and require assurances that the organization will comply with PHI privacy

[4] U.S. Department of Health and Human Services, HHS.gov, Minimum Necessary Requirement, www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html.

and security regulations. For more information on HIPAA and 42 CFR Part 2 permitted contractual agreements and a sample agreement to use as a starting point to develop such agreements, refer to Appendix D.

III. Who Should Use This Resource?

This resource was designed to be used by correctional entities that are "covered entities" (see Chapter 2, section I. A.) **and/or "federally assisted programs"** (see Chapter 2, section II. A.) to enable them to build PHI privacy frameworks in compliance with HIPAA and 42 CFR Part 2 for the receipt or sharing of PHI. However, this resource is also designed to be used by **any** correctional entity interested in articulating its commitment to protecting privacy in the entity's PHI-handling process, whether or not the entity is a covered entity and/or a federally assisted program. When receiving or sharing PHI, entities are strongly encouraged to have PHI privacy frameworks in place to provide explicit and detailed privacy protection guidance to entity personnel and other authorized source, user, and participating agencies.

IV. Tools in Appendix

Useful tools are included in the appendices of this template to assist corrections entities in their privacy policy drafting processes, development of consent authorization forms, establishment of contractual agreements with outside organizations, drafting of language for court orders, policy evaluation checklist to ensure that policies are legally compliant, and follow-up research efforts on the subjects contained within this document.

- **Appendix A: Glossary of Terms and Definitions**
- **Appendix B: Listing of Applicable Federal Laws**
- **Appendix C: Release of Information: Consent Authorization Guidance**
- **Appendix D: Contractual Agreements**
- **Appendix E: Court Orders**
- **Appendix F: 42 CFR 2.22: Notice to Patients of Federal Confidentiality Requirements**
- **Appendix G: PHI Privacy Policy Review Checklist**
- **Appendix H: Standards and Resource List**
- **Appendix I: Acknowledgments**

Chapter 2: Overview of HIPAA and 42 CFR Part 2 Regulations

I. Overview of HIPAA Regulations—Medical and Mental Health Information

It should be noted that HIPAA was designed for and meant to facilitate the sharing of information. HIPAA's restrictions on sharing health information are often misunderstood. This often results in practitioners and their respective legal counsel applying restrictions to information sharing that are far more restrictive than the actual regulatory language requires. Though this template is not intended to be a primer on HIPAA and 42 CFR Part 2 information, the following is a brief overview of each regulation. For more information on these regulations and how they relate to the corrections environment, refer to the standards and resources listed in Appendix G.

The Secretary of the U.S. Department of Health and Human Services (HHS) developed regulations protecting the privacy and security of certain health information through the HIPAA Privacy Rule.[5] The Privacy Rule, or *Standards for Privacy of Individually Identifiable Health Information* (term modified in 2013 to Protected Health Information), establishes national standards for the protection of certain health information.

The Privacy Rule requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information **without patient authorization**. Though generally an authorization will be required if the information is to be shared for the purposes of treatment, payment, or health-care operations, consent **can be** obtained from the individual **but is not necessarily required** under HIPAA. Although HIPAA does not require consent in these situations, state law may.[6] The rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections.

HIPAA is not an insurmountable barrier to justice-health information sharing. However, a general lack of understanding of the requirements of HIPAA and fear of violating privacy regulations can act as obstacles to effective interagency collaboration.[7]

[5] U.S. Department of Health and Human Services (HHS), HHS.gov, Health Information Privacy, The Privacy Rule, www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html.

[6] *Information Sharing in Criminal Justice—Mental Health Collaborations: Working with HIPAA and Other Privacy Laws*, John Petrila, J.D., L.L.M, and Hallie Fader-Towe, J.D., Council of State Governments Justice Center, Bureau of Justice Assistance, Office of Justice Programs, DOJ, www.bja.gov/Publications/CSG_CJMH_Info_Sharing.pdf.

[7] Toolkit, Legal and Ethical Regulations, Justice and Health Connect, Substance Use and Mental Health Program at the Vera Institute of Justice, supported by the Department of Justice's (DOJ) Bureau of Justice Assistance, www.jhconnect.org/toolkit#module-3-map-legal-and-ethical-regulations.

A. HIPAA-Covered Entities

HIPAA's restrictions on sharing health information are often misunderstood, which has resulted in practitioners misapplying the law to be far more restrictive than the actual regulatory language requires. HIPAA sets out rules governing how entities, which are identified as "**covered entities**," share PHI. It is important to note that the HIPAA Privacy Rule applies only to the use and disclosure of PHI by covered entities. This means that HIPAA applies if either the entity **requesting** information or the entity **providing** information is a covered entity. As such, correctional institutions will need to first assess whether they are covered entities to determine whether they must comply with HIPAA. A covered entity is defined as:

- A health plan;
- A health clearinghouse; or
- A health-care provider that transmits any health information in electronic form in connection with a transaction [relating to health claim report, status, payment, etc.] [9]

Entities may find the following covered entity decision tool useful in determining whether they are covered entities. The tool is located at www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf. To use this tool to determine whether a person, business, or government agency is a covered entity, refer to the tool's chart(s) that apply to the person, business, or agency and answer the questions, starting at the upper left-hand side of the chart(s).

In accordance with 45 CFR Part 164 Subpart C § 164.506, a HIPAA-covered entity may use or disclose PHI for its own treatment, payment, or health-care operations without requiring individual authorization, except for disclosures described in § 164.508.

Covered Entities:
When Consent Is Not Required[8]

Treatment, payment, or health-care operations—HIPAA permits covered entities to transmit PHI without consent and provides entities with the necessary level of discretion to share PHI and carry out routine health-care delivery. It applies to entities in charge of coordinating treatment, performing case management, processing payments, and improving the quality of care in a facility.

Public health activities—This provision permits reporting statistics that allow entities to compile population levels of certain diseases (i.e., disease prevention, surveillance, and control).

Court orders and subpoenas—Covered entities can disclose PHI when required by an order or a subpoena from a court or administrative agency. The order must clearly describe the information being sought and the purpose, and only that information specifically described can be disclosed.

Law enforcement purposes—Covered entities can disclose limited information to police agencies when necessary to identify or locate suspects, fugitives, or victims; to investigate a crime; and in response to emergency situations in which someone is at risk of serious injury. The entity also may release such information if an individual admits to committing a violent crime and the entity believes the person may have caused serious physical harm to the victim; or when there is an instance of suspected abuse or neglect of a child or disabled person. See section E.a. for more information.

Deidentified data—Consent is not required if PHI is deidentified and used for research purposes. HIPAA provides a set of rules and standards for deidentifying data.

a. HIPAA Required Risk Assessment

In accordance with 45 CFR Part 164 Subpart C § 164.308, Administrative Safeguards, **a covered entity is required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities** to the confidentiality, integrity, and availability of electronic PHI held by the covered entity and must implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a). The results of this risk assessment will help to inform the provisions of the entity's privacy protections policy covering PHI.

[8] *The HIPAA Privacy Rule*, Justice and Health Connect, Substance Use and Mental Health Program at the Vera Institute of Justice, supported by the Department of Justice's (DOJ) Bureau of Justice Assistance, www.jhconnect.org/wp-content/uploads/2013/06/HIPAA-FINAL.pdf.

[9] 45 CFR Part 160 General Administrative Requirements, Subpart A, § 160.103 Definitions, www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf.

B. Correctional Institutions Which Are HIPAA-Covered Entities[10]

Since corrections entities generally do not process or facilitate the processing of health information, and their principal purpose is not providing or paying for the cost of health care, a corrections entity's status as a covered entity may depend on its qualification (or lack thereof) as a health-care provider which transmits health information in electronic form in connection with a **covered transaction**. That is, if the entity **furnishes health care**, bills, or is paid for health care in the normal course of business **and transmits information in electronic form** in connection with **one of the following** eight types of **covered transactions**, **the corrections entity meets the criteria of a covered entity and must comply with HIPAA.**

Covered transactions:

- Health-care claims or equivalent encounter information
- Eligibility for a health plan
- Referral certification and authorization
- Health-care claim status
- Enrollment and disenrollment in a health plan
- Health-care payment and remittance advice
- Health plan premium payments
- Coordination of benefits

Although corrections entities are not likely to engage in most of the transactions above, **it is conceivable that a corrections entity might transmit clinical encounter information for the purpose of**:

- Reporting health care.
- Requesting a review of health care in order to secure an authorization.
- Receiving payment of health-care claims from a private or public health plan.

In addition, if the correctional entity electronically transmits any one of these covered transactions or has a contract with another provider that electronically transmits the health-care information, the corrections entity does meet the criteria as a covered entity and will be required to comply with HIPAA. Finally, even if correctional entities contract out relevant health-care services, the corrections entity must comply with HIPAA.

Lawful Custody[11]

HIPAA does not preclude information sharing between health and justice systems. Generally, HIPAA allows covered entities, such as health-care providers, to share PHI with correctional facilities when a person is in custody and doing so is necessary to permit continuity of care. While it is always best to obtain consent when feasible, HIPAA does provide an exception to allow sharing between health-care providers and correctional facilities.

HIPAA's "lawful custody exception" provides that when a correctional institution or law enforcement agency has custody of an individual, HIPAA permits access to PHI without consent if the information is necessary to (1) provide health care to the individual; (2) ensure the health and safety of the inmate or others housed or working in the facility; (3) protect the health and safety of any law enforcement officer transporting an inmate between facilities; (4) protect those involved in the transfer or transporting of the individual; (5) promote law enforcement on the premises of the correctional institution; or (6) maintain and administer safety, security, and good order in the correctional facility. See 45 CFR 164.512(j)(1)(ii)(B)).

The lawful custody exception, however, no longer applies once a person is released from custody, including on probation or parole.

[10] *Health Information Privacy in the Correctional Environment*, Melissa M. Goldstein, JD, The George Washington University, Issue Paper, Community Oriented Correctional Health Services, April 2012, www.cochs.org/files/hieconf/PRIVACY.pdf.

[11] *The HIPAA Privacy Rule*, Justice and Health Connect, Substance Use and Mental Health Program at the Vera Institute of Justice, supported by the Department of Justice's (DOJ) Bureau of Justice Assistance, www.jhconnect.org/wp-content/uploads/2013/06/HIPAA-FINAL.pdf.

a. HIPAA Privacy Policy Provisions Within This Resource

As mentioned in Chapter 1, Section II. PHI Privacy Framework, this resource contains a PHI privacy policy template in Chapter 3 which features guidance and HIPAA- and 42 CFR Part 2-compliant sample policy language for entities to use when drafting a PHI privacy policy. Correctional institutions that have been determined to be HIPAA-covered entities must comply with HIPAA regulations. To assist with this mandate, the policy template lists HIPAA requirements throughout the template, where applicable, alongside relevant privacy policy questions and sample language.

Correctional institutions that do **not** fall under the HIPAA definition of a covered entity, may still receive PHI in accordance with 45 CFR Part 164 Subpart C § 164.512(k)(5), as explained below in section D., Correctional Institutions Which Are Not HIPAA-Covered Entities.

C. HIPAA Disclosure Permissions Do Not Guarantee Sharing

It is important to note that while the HIPAA Privacy Rule permits disclosures without authorization in the circumstances described in section D., **such disclosures are not required** by the Rule; that is, a covered entity could choose not to disclose the information at issue or to seek the individual's authorization to do so. See section II. F. for a similar provision regarding substance abuse information.

D. Correctional Institutions Which Are Not HIPAA-Covered Entities

If a corrections entity is self-insured and self-pays and does not engage in standard transactions, it might be exempted from covered entity status. This could also be the case if an institution has a contract with a third party to provide health care but participates in no billing using the electronic standards.

Beyond the question of whether a correctional facility is or is not a covered entity, HIPAA will have an impact on correctional institutions and their ability to receive PHI from covered entities, such as community health-care agencies, hospitals, etc.

a. Sharing PHI With Correctional Institutions

HIPAA considers the medical and mental health information of prisoners to be PHI to the extent that it otherwise meets the definition of such and is maintained or transmitted by a health care agency that is a covered entity. However, through 45 CFR Part 164 Subpart C § 164.512(k)(5), "Correctional institutions and other law enforcement custodial situations," HIPAA recognizes that correctional facilities have legitimate needs for the use and sharing of inmates' PHI **without the written authorization of the individual** [inmate] or the opportunity for the individual to agree or object for the following specialized functions.

HIPAA-covered entities are permitted to disclose PHI **without written authorization** of the individual **to a correctional institution** or other law enforcement official having **lawful custody** of an inmate or other individual when the PHI is about such inmate or individual and if the correctional institution or such law enforcement official represents that such PHI is necessary for:

- The provision of health care to such individuals.
- The health and safety of such individual or other inmates.
- The health and safety of the officers or employees of or others at the correctional institution.
- The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another.
- Law enforcement on the premises of the correctional institution.
- The administration and maintenance of the safety, security, and good order of the correctional institution.

Similar to HIPAA's "lawful custody" exception, state law may permit community health providers to share specific types of clinical information with a correctional facility or a corrections officer who is responsible for

the supervision of a person who is receiving inpatient or outpatient evaluation or treatment.[12] Corrections entities are guided to consult their state laws or legal counsel to determine whether state regulations permit this type of sharing.

b. Sharing PHI With Pre-Trial, Probation, and Parole

HIPAA's permitted disclosure of inmate PHI without written authorization **does not apply** to individuals who are released from prison, or to those in pre-trial release or on probation or parole, since they no longer fall into the category of lawful custody. **When individuals are released from a correctional facility, they have the same privacy rights under HIPAA's Privacy Rule that apply to all other individuals, and covered entities must apply privacy protections and restrictions to PHI without the exceptions outlined specifically for inmates. As such, covered entities that may have previously shared PHI with a correctional institution when the individual was in lawful custody must now require the individual's written authorization to share PHI.** Further, these rules apply equally to all covered entities, including those that are health-care components of a correctional institution (such as a prison clinic) and those that provide services to inmates under contract to correctional institutions. In these situations, a written authorization would need to be obtained from the individual (see Appendix C) in order to disclose his or her PHI. Pre-trial, probation, and parole officers are not covered entities and therefore are not bound by HIPAA when asked to provide PHI to others except in certain limited circumstances (e.g., pursuant to a protective court order). **For a supervising officer to receive PHI, the released individual must give permission** (such as a written authorization [see Appendix C]) **or a court must include a provision in the conditions of release that permit the supervising officer to obtain PHI when necessary to monitor compliance** (see Appendix E).

Further, HIPAA does not prohibit redisclosure of PHI by a noncovered entity. For example, if a former inmate discloses PHI to his/her probation officer, the officer may share or redisclose the information to law enforcement without adhering to HIPAA requirements, assuming no state law prohibits such disclosure. Since state law might place restrictions on the disclosure of PHI, entities are encouraged to become familiar with the requirements of their state laws.

E. Other Criminal Justice Entities Which Are Not HIPAA-Covered Entities

In the criminal justice context, certain stakeholders (for example, law enforcement, courts, defense lawyers, and prosecutors) clearly are not covered entities. As such, they are not bound by HIPAA when asked to provide PHI to others except in certain limited circumstances (e.g., pursuant to a protective court order).

a. Sharing PHI With Law Enforcement[13]

HIPAA-covered entities are permitted to disclose PHI without the written authorization of the individual or the opportunity for the individual to agree or object for **law enforcement purposes to a law enforcement official**,[14] but only:

- If required by laws that require reporting of certain types of wounds or physical injuries;
- In compliance with and as limited by the relevant requirements of a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, a grand jury subpoena, or an administrative request, or a civil or an authorized investigative demand, authorized under law, provided the information sought is relevant and material to a legitimate law enforcement inquiry, specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought and deidentified information could not reasonably be used.

[12] *A Quick Guide to State Laws on Sensitive Health Information*, Justice and Health Connect, Substance Use and Mental Health Program at the Vera Institute of Justice, supported by the Department of Justice's (DOJ) Bureau of Justice Assistance, www.jhconnect.org/wp-content/uploads/2013/06/State-Health-Laws-fact-sheet-June-23-2013.pdf.

[13] The HIPAA Privacy Rule, Justice and Health Connect, Substance Use and Mental Health Program at the Vera Institute of Justice, supported by the Department of Justice's (DOJ) Bureau of Justice Assistance (BJA), www.jhconnect.org/wp-content/uploads/2013/06/HIPAA-FINAL.pdf.

[14] *When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement?*, U.S. Department of Health and Human Services (HHS), www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_for_law_enforcement_purposes/505.html.

- For purposes of identifying or locating a suspect, fugitive, material witness, or missing person, provided the entity only discloses the information listed in § 164.512 (f)(2)(i) but the covered entity may not disclose PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

- As part of a law enforcement official's request about an individual who is or is suspected to be a victim of a crime, if the individual agrees to the disclosure or the covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that the law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure, and disclosure is in the best interest of the individual as determined by the covered entity.

- For the purpose of alerting law enforcement of the death of the individual if the covered entity suspects the death may have resulted from criminal conduct.

- If the entity believes in good faith that the PHI constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

- If providing emergency health care in response to a medical emergency, the entity may disclose PHI to a law enforcement official if disclosure appears necessary to alert law enforcement to the commission and nature of a crime, the location of such crime, or the victim(s) of such crime, and the identity, description, and location of the perpetrator of such crime or the entity believes the PHI is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care.

b. Sharing PHI for Other Criminal Justice Activities

HIPAA also permits a range of other uses and disclosures of PHI without individual consent, authorization, or agreement that are relevant to criminal justice activities. Such permitted disclosures include those related to public health activities; judicial and administrative proceedings; certain law enforcement purposes; those necessary to avert a serious threat to health or safety; to report potential abuse, neglect, or domestic violence to government authorities; and disclosures by law. In all of these scenarios, HIPAA may permit the disclosures within certain parameters but does not require them. **Covered entities are always free to seek the individual's consent and authorization, or to choose not to disclose the information. This is an important point for consideration: Simply because an entity may not be required to seek an individual's consent, that does not mean that it necessarily should not seek their consent. This is an ethical and fundamental decision that entities will need to consider when choosing how to conduct their businesses, regardless of the legally binding issues mentioned herein.** Also, state law must be consulted on this as well. If state law provides more protection for the PHI in any particular circumstance than does HIPAA, then the state law applies (unless it contradicts HIPAA[15]).

HIPAA does allow a covered entity to use or disclose PHI without authorization if the covered entity believes, in good faith, that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

A covered entity also may disclose PHI without written authorization in response to an order of a court or administrative tribunal, provided that the covered entity discloses only the PHI expressly authorized by the order. In the absence of a court order, a covered entity may disclose PHI in response to a subpoena, discovery request, or other lawful process if the covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to give notice of the request to the individual who is the subject of the PHI or that reasonable efforts have been made to attain a qualified protective order for the PHI.

[15] Preemption provisions of the HIPAA Rules are based on section 1178 of the Social Security Act. Through these statutory provisions, Congress made clear that the HIPAA privacy requirements are to supersede only "**contrary**" provisions of state law. Accordingly, the HIPAA Privacy Rule provides a federal floor of privacy protections, with states free to impose more stringent privacy protections should they deem it appropriate.

c. Sharing PHI For Specialized Government Functions

HIPAA-covered entities are permitted to disclose PHI without the written authorization of the individual or the opportunity for the individual to agree or object for specialized government functions, such as to **authorized federal officials** for the conduct of lawful intelligence, counterintelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority.

II. Overview of 42 CFR Part 2—Substance Abuse Information

Note: The term "substance abuse," in the current law (42 U.S.C. § 290dd-2) and within this template, refers to both alcohol and drug abuse**.**

For entities that handle substance abuse testing and treatment, an additional set of federal regulations, Confidentiality of Substance Abuse Patient Records, Code of Federal Regulations, Title 42: Public Health, Part 2, (42 CFR Part 2)[17] applies to those institutions which are "federally assisted" providers that meet the definition of a "program" (or "**federally assisted program**").

The Basics of 42 CFR, Part 2[16]

Requires specific consent—With certain conditions and exceptions, Part 2 prohibits the disclosure and use of substance use treatment records without a person's specific consent. It is stricter than HIPAA in that Part 2 **does not** have an explicit treatment exception that allows care providers to share information without consent when the purpose is to coordinate treatment.

Applies to most providers—Part 2 applies to substance use treatment programs that receive any form of federal assistance (e.g., grant funding, Medicaid).

Applies to identifiable information—These regulations apply broadly to any information that can be used to identify an individual as someone seeking or receiving care for substance use.

Has limited exceptions to consent requirement—Part 2 defines limited circumstances where disclosures can be made without consent, including medical emergencies, research, and audits or evaluations.

Sets a floor—Similar to HIPAA, Part 2 sets a federal privacy floor, meaning it preempts state laws that are less protective of substance use information privacy but preserves provisions of state law that are more stringent.

A. Federally Assisted Programs

A **program** includes any individual or entity (other than a general medical care facility) that holds itself out as providing, in whole or in part, substance abuse diagnosis, treatment, referral for treatment or prevention[18] (42 U.S.C §§ 290dd-2, 42 CFR 2.11); or an identified unit within a general medical facility that holds itself out as providing, and provides, substance abuse diagnosis, treatment, referral for treatment, or prevention; or medical personnel or other staff in a general medical facility whose primary function is the provision of substance abuse diagnosis, treatment, referral for treatment, or prevention, and who are identified as such providers (see 42 CFR Part 2 Subpart B § 2.12(e)(1) for examples).

42 CFR Part 2 regulations, however, do not, for example, apply to emergency room personnel who refer a patient to the intensive care unit for an apparent overdose, unless the primary function of such personnel is the provision of substance abuse diagnosis, treatment, referral for treatment, or prevention and they are identified as providing such services; or the emergency room has promoted itself to the community as a provider of such services.

A program is **federally assisted** if it:

- Receives federal funds **in any form**, whether or not the funds directly pay for substance abuse services.
- Is being carried out under a license, certification, registration, or other authorization granted by the federal government (e.g., licensed to provide methadone, certified as a Medicare provider).

[16] Federal Privacy Law, Legal and Ethical Regulations, Toolkit, Justice and Health Connect, Substance Use and Mental Health Program at the Vera Institute of Justice, supported by the Department of Justice's (DOJ) Bureau of Justice Assistance, www.jhconnect.org/toolkit#module-3-map-legal-and-ethical-regulations.

[17] Confidentiality of Substance Abuse Patient Records, Code of Federal Regulations, Title 42: Public Health, Part 2 (42 CFR Part 2).

[18] There has been some discussion as to whether prevention programs are covered by 42 CFR Part 2, since the original regulations themselves did not specifically mention prevention programs. However, the current federal authorizing statute for the regulations (47 U.S.C. § 290dd-2) and the original authorizing statues (42 U.S.C. §§ 290dd-2 and 290ee-3), which are now incorporated into the regulations, explicitly state that prevention programs and activities are covered.

- Is assisted by the Internal Revenue Service through a grant of tax-exempt status or allowance of tax deductions for contributions.
- Is conducted directly by the federal government or by a state or local government that receives federal funds which could be (but are not necessarily) spent for substance abuse programs.

B. 42 CFR Part 2 Restrictions on Disclosure and Use

Whether a 42 CFR Part 2 restriction covers use or disclosure affects the type of information which may be available.

- **The restriction on disclosure** applies to **any** record of the identity, diagnosis, prognosis, or treatment of any patient which is maintained in connection with the performance of any substance abuse prevention function conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall, except provided in § 290EE-3 (e) (Armed Forces and Veterans' Administration records), be confidential and be disclosed only for the purposes and under the circumstances prescribed (in this regulation). Therefore, prevention efforts are covered under 42 CFR Part 2 if sharing the information would disclose that an individual is a substance abuser or is in an alcohol or drug program. As an example, a general drug and alcohol education class for an entire inmate population would not be covered under 42 CFR Part 2, whereas a class that targets a specific audience, such as inmates who have been caught with or who are known to have used drugs, would be covered under 42 CFR Part 2. The prohibition continues to apply to records concerning any individual who has been a patient, irrespective of whether or when such individual ceases to be a patient (including inmates and those released from incarceration).

  The restriction on use of substance abuse information, per 42 CFR Part 2 Subpart B § 2.12(d), refers to a restriction to initiate or substantiate any criminal charges against a patient or to conduct any criminal investigation of a patient by any person who obtains that information from a federally assisted substance abuse program, regardless of the status of the person obtaining the information or of whether the information was obtained in accordance with these regulations. This restriction on use bars, among other things, the introduction of that information as evidence in a criminal proceeding and any other use of the information to investigate or prosecute a patient with respect to a suspected crime. Information obtained by undercover agents or informants (see § 2.17) or through patient access (see § 2.23) is subject to the restriction on use. Subpart B § 2.12 (e)(3) applies to any information obtained by the program for the purpose of diagnosis, treatment, or referral of treatment of substance abuse and restricts the use of that information in criminal charges against a patient for a crime.

If an entity is covered under both HIPAA and 42 CFR Part 2, the statute that is **more protective (most restrictive) of the patient's information must be followed**.

C. Disclosure of Substance Abuse Information Requiring Patient Consent

Apart from the exceptions listed in D., below, an individual's written authorization must be used for any authorized disclosure of substance abuse information. The consent form, per 42 CFR Part 2, must contain certain elements to be valid, including the purpose of the disclosure, the name of the person/entity that is to receive the information, a date or condition upon which the consent expires, and a specific regulation-stated prohibition on redisclosure.[19] **42 CFR Part 2 prohibits anyone who receives information from a substance abuse program from redisclosing it and requires that any information released must be accompanied by a written notice informing the recipient that federal law prohibits its redisclosure unless expressly permitted by the patient or as otherwise authorized by the regulations.** For more information on the specific elements of an authorization 42 CFR Part 2 requires, refer to Appendix C. The best way to ensure that communications are permissible under this regulation, as well as HIPAA, is to have the individual provide written authorization to release information that complies with the requirements of both HIPAA and 42 CFR Part 2. For a sample consent authorization form that incorporates both of these regulations' required elements, refer to Appendix C.

D. Disclosure of Substance Abuse Information Without Requiring Patient Consent

While HIPAA provides exemptions where specific use and disclosures of PHI do not require individual authorization, **nearly all PHI disclosures allowed under 42 CFR Part 2 require specific patient consent**. 42

[19] *Health Information Privacy in the Correctional Environment*, Melissa M. Goldstein, JD, The George Washington University, Issue Paper, Community Oriented Correctional Health Services, April 2012, http://www.cochs.org/files/hieconf/PRIVACY.pdf.

CFR Part 2's prohibition on disclosing PHI has very few exceptions. The following are the general categories of exceptions where disclosure is allowed without patient consent:

- Internal program communications (including communications within a program or between a program and an entity having direct administrative control over that program [e.g., the staff of a detoxification unit within a hospital can share information with hospital administrators where needed to provide substance abuse services to the program's patients])
- Removal of all patient identifying information
- Medical emergency[20,21]
- Court order with subpoena regarding a crime that has occurred on the program's premises or against program personnel
- Scientific research
- Audits and evaluations
- Child abuse
- In conjunction with a qualified service organization agreement (QSOA). A QSO is a person or entity that provides services such as data processing, bill collection, or accounting to a program, as part of a QSOA, when the information exchange is needed to provide the covered services. See III. Contractual Agreements and Appendix D for more information.

E. Sharing Substance Abuse Information With Criminal Justice Entities

Although the HIPAA Privacy Rule contains specific disclosure provisions for correctional institutions and law enforcement, 42 CFR Part 2 does not. Corrections and law enforcement officials, in order to obtain substance abuse information from a 42 CFR Part 2 program, will likely require court orders. In addition, **disclosure of 42 CFR Part 2 information to or from a correctional facility will most likely require patient consent or a court order**.

42 CFR Part 2 does, however, make explicit allowance for disclosures **within the criminal justice system**. In accordance with 42 CFR Part 2 Subpart C § 2.35, a program may disclose information about a patient to those persons within the criminal justice system who may have made participation in the program a condition of the disposition of any criminal proceedings against the patient (e.g., as part of a drug court program or other treatment-based alternative to incarceration) or a condition of the patient's parole or other release from custody if:

- The disclosure is made only to those individuals within the criminal justice system who have a need for the information in connection with their duties to monitor the patient's progress (e.g., a prosecuting attorney who is withholding charges against the patient, a court granting pre-trial or post-trial release, **probation or parole officers responsible for supervision of the patient**); **and**
- The **patient has signed a written consent** that meets the requirements of § 2.31 (form of written consent, except (a)(8) regarding revocation) and also states a reasonable period during which it remains in effect, taking into consideration the anticipated length of treatment, type of criminal proceeding involved, and need for information in connection with the final disposition of that proceeding and when the final disposition will occur, and other pertinent factors.

[20] Part 2 does not distinguish between physical and mental health emergencies. A medical emergency is simply defined, per 42 CFR Part 2 Subpart D § 2.51(a), as a health emergency affecting any individual who requires immediate medical intervention.

[21] Per 42 CFR Part 2 Subpart B § 2.13(a) and in contrast to circumstances where information is disclosed through patient consent, if a medical emergency exists. Part 2 provisions do not prohibit the redisclosure of Part 2 information once it is released. Consequently, medical personnel treating a patient for a medical emergency who are affiliated providers may download and include in their own records the information they obtained in treating the emergency, and may then redisclose that information to others without obtaining patient consent. However, all disclosures of information under the regulation must be limited to the information necessary to carry out the purpose of the disclosure.

The written consent must state that it is revocable upon the passage of a specified amount of time or the occurrence of a specified, ascertainable event and may be no later than the final disposition of the conditional release or other action in connection with which consent was given.

Anyone who receives patient information under this provision of 42 CFR Part 2 (such as a probation officer) may redisclose and use it only to carry out that person's official duties with regard to the patient's conditional release or other action in connection with which the consent was given.

F. 42 CFR Part 2 Disclosure Permissions Do Not Guarantee Sharing of PHI

Similar to the HIPAA provision described in section I.C., in which provider disclosures are not required even if HIPAA regulations are met, 42 CFR Part 2 has a similar provision. In accordance with 42 CFR Part 2 Subpart C § 2.3(b), the disclosure requirements and exceptions contained in 42 CFR Part 2 regulations **do not compel disclosure**. Thus, **42 CFR Part 2 regulations do not require disclosure under any circumstances, whether disclosure conditions have been met or not.**

G. Sharing Substance Abuse Information by Programs That Are Not Federally Assisted

In accordance with 42 CFR Part 2 Subpart B § 2.12(e)(2), if a patient's substance abuse diagnosis, treatment, or referral for treatment is not provided by a program which is federally conducted, regulated, or supported in a manner which constitutes federal assistance under § 2.12(b), that patient's record is NOT covered by these regulations. As such, **if the individual received treatment prior to entering incarceration, while incarcerated, or following supervised release from a program that is not federally assisted, then the individual's record held by that program would not have to meet the confidentiality regulations of 42 CFR Part 2**.

42 CFR Part 2 and Criminal Justice[22]

Police—Generally, without consent, police officers need a court order to obtain PHI from a substance use treatment provider, except for two scenarios: medical emergency or a crime committed on the premises of the treatment facility.

Court orders—Absent consent, a court order will generally be required to receive PHI from a substance use program, §§.2.61-67. Court orders are granted only when disclosure is needed to protect against an existing threat to life or serious bodily injury or is necessary for further investigation of a serious crime.

Prosecutors, defenders, and the courts—Courts and lawyers are not federally assisted programs; however, court appearances are frequently used to divert people from incarceration to treatment programs. 42 CFR Part 2 has a provision for when criminal justice entities, such as drug courts or diversion programs, make referrals to treatment providers as a conditional disposition. This allows programs to share PHI with the court (or other entity tasked with monitoring progress), with the individual's consent, § 2.35. Courts have upheld that it is constitutional to require confidentiality waivers as a condition of participating in a drug court.

Jails and prisons—42 CFR Part 2 does NOT permit PHI about substance abuse to flow to or from a correctional facility without an individual's consent.

Community corrections—Probation and parole officers are not federally assisted programs. As such, they can disclose PHI they learn by interviewing clients to others. However, they cannot request and receive PHI from programs without prior, valid consent. If a probation or parole officer needs PHI, courts can require a waiver of confidentiality for both substance use and mental health information as a condition of release from prison or probation.

H. Diagnoses Not Covered by 42 CFR Part 2

42 CFR Part 2 covers any record of a diagnosis which identifies a patient as a substance abuser and is prepared in connection with the treatment or referral for treatment of substance abuse. A diagnosis prepared for the purpose of treatment or referral for treatment but which is not so used is also covered by these regulations. In accordance with 42 CFR Part 2 Subpart B § 2.12(e)(4), the following are **diagnoses which are not covered by 42 CFR Part 2 regulations**:

- Diagnosis which is made solely for the purpose of providing evidence for use by law enforcement authorities (for example, a blood alcohol content test performed by a federally assisted program but performed at the request of law enforcement during its criminal investigation, not for the purpose of treatment); or

[22] *Basics of 42 CFR, Part 2*, Justice and Health Connect, Substance Use and Mental Health Program at the Vera Institute of Justice, supported by the Department of Justice's (DOJ) Bureau of Justice Assistance, www.jhconnect.org/wp-content/uploads/2013/06/42-CFR-Part-2-final.pdf.

- A diagnosis of drug overdose or alcohol intoxication which clearly shows that the individual involved is not a substance abuser (e.g., involuntary ingestion of alcohol or drugs or reaction to a prescribed dosage of one or more drugs).

III. Contractual Agreements

Pursuant to both HIPAA and 42 CFR Part 2, entities can disclose PHI, without individual consent, to outside organizations that perform certain functions or provides services to the entity, by establishing contractual agreements. HIPAA calls these agreements "Business Associate Agreements"—or BAAs while 42 CFR Part 2 uses the term "Qualified Service Organization Agreements"—or QSOAs. BAAs and QSOAs, while very similar in contractual requirements, each have their own set of criteria for what constitutes a business associate or a qualified service organization and the conditions by which a contractual agreement would be permitted. For more information on HIPAA and 42 CFR Part 2 permitted contractual agreements and a sample agreement to use as a starting point to develop such agreements, refer to Appendix D. Contractual Agreements.

IV. State Law Versus HIPAA and 42 CFR Part 2

While HIPAA and 42 CFR Part 2 establish minimum standards for protecting and securing PHI and patient identifying information, the two regulations rarely explicitly prohibit the sharing of information. Rather, they generally provide guidance about the conditions under which information may be shared. However, there are important differences, with HIPAA typically being more permissive about information sharing than 42 CFR Part 2. Like HIPAA, 42 CFR Part 2 sets a federal privacy floor. State laws that are less protective regarding disclosure and use of information about individuals in federally assisted substance abuse treatment programs are preempted, while state laws that are more stringent are preserved. In cases where state law is contrary to HIPAA,[23] the rules under HIPAA prevail. However, if state law is more stringent than HIPAA without presenting a conflict, state law takes precedence. Refer to the definition of "Contrary" in Appendix A. Terms and Definitions. Further, HIPAA generally defers to state law regarding minors' rights issues with respect to the disclosure of a minor's PHI. It is recommended that entities research prevailing state law on minors' rights (such as age of maturity) and include this information in the entity's privacy policy.

Entities are encouraged to review their state laws. If state law is more restrictive (i.e., is more protective of privacy) than HIPAA or 42 CFR Part 2, then the state law governs.

[23] Preemption provisions of the HIPAA Rules are based on section 1178 of the Social Security Act. Through these statutory provisions, Congress made clear that the HIPAA privacy requirements are to supersede only "**contrary**" provisions of state law. Accordingly, the HIPAA Privacy Rule provides a federal floor of privacy protections, with states free to impose more stringent privacy protections should they deem appropriate.

Chapter 3: PHI Policy Development Template

The policy provisions contained in this template are provided to assist corrections entities in developing PHI privacy policies related to the medical, mental health, and, if applicable, substance abuse testing and treatment information the entities collect, receive, maintain, archive, access, and disclose to entity personnel; government agencies; participating criminal justice and public safety agencies; private contractors; as well as community medical, mental health, and substance abuse treatment providers, and the general public. Each section of the template comprises a fundamental component of a comprehensive policy that includes baseline provisions on information collection, information quality (IQ), collation and analysis, merging of records, information access and disclosure, redress, security safeguards, retention and destruction, accountability and enforcement, and training.

The template is structured in a question-and-answer format to enable policy authors, prompted by key policy questions, to draft policy language that addresses each question posed. Policy questions are shown in **bold type** and are grouped according to related policy concepts (or sections). Following each question is sample language (in regular type) to help policy authors understand the meaning of the question asked and to illustrate how to write policy language that addresses the policy question (e.g., formulate privacy policies).

Sample Language—It is important to note that the sample language which follows each question is not intended to be used as is without modification. Entities are strongly encouraged to use the sample language as a starting point and to customize policy language to ensure it is applicable to the specific entity. In addition, while this template represents the foundational components of an effective PHI privacy policy, it does not cover all concepts that may be particular to your entity, its unique processes and procedures, or the specific constitutional provisions, laws, ordinances, or regulations established within your state. Further, there may be certain policy questions within this template that simply may not apply to your entity.

This template was designed to establish **minimum** baseline PHI privacy protections. Corrections entities are guided to complete as many of the template questions as are applicable and to enhance sections with references to applicable statutes, rules, standards, or policies and to provide additional sections for provisions that are not addressed within this template. **Please note: This template does not constitute legal guidance, and users should consult their counsel to ensure that their policies meet all federal and state requirements.**

Referencing Other Policies—In many cases, entities may already have established privacy-related policies and practices described in broader policy documents (e.g., concept of operations, standard operating procedures, and employee handbooks). In accordance with template Sections N, Accountability and Enforcement, and N.1, Information System Transparency, entities are strongly encouraged to make their privacy policies available to the public, even if the other existing policies are not made publicly available. As such, consolidating existing PHI policies into one PHI privacy policy is highly recommended. Entities are cautioned, however, against simply providing a cross-reference to other policies in effect. Cross-referencing, without including the applicable policy language, should be done only if those policies are also available to the public; otherwise, entities should restate or excerpt the applicable language within their PHI privacy policies.

HIPAA and 42 CFR Part 2 Citations—The privacy policy provisions outlined within this template and the tools provided in its appendices were developed specifically for the receipt and/or disclosure of medical, mental health, and substance abuse information. As such, the template questions and sample language include, where applicable, citations to HIPAA Privacy and Security Rule regulations, as well as to 42 CFR Part 2 requirements. Refer to Chapter 2 for an overview of HIPAA and 42 CFR Part 2 regulations.

A. Purpose Statement

1. What is the purpose of establishing a privacy, civil rights, and civil liberties protection policy (i.e., what does the entity hope to accomplish in adopting this policy)? Provide a succinct, comprehensive statement of purpose.

SAMPLE LANGUAGE, EXAMPLE 1: The purpose of this policy is to establish privacy, civil rights, and civil liberties protections that can be used by the corrections community to develop lawful and effective medical, mental health, and substance abuse information exchanges between and among law enforcement; public safety; health and mental health providers; human/social services agencies, including substance abuse treatment agencies, and other government and community organizations that need information about individuals involved in the justice system to ensure continuity of care and participate effectively in the pre- and post-adjudication processes without compromising individual rights. The **[name of entity]** will protect the civil and legal rights of each individual in the entity's corrections population.

SAMPLE LANGUAGE, EXAMPLE 2: The purpose of this policy is to promote agency conduct that complies with applicable federal, state, local, and tribal laws, regulations, and policies and assists all parties in:

- Developing lawful and effective medical and behavioral health information exchanges between and among law enforcement; public safety; health and mental health providers; human/social services agencies, including substance abuse treatment agencies; and other government and community organizations that need information about individuals involved in the justice system to ensure continuity of care and participate effectively in the pre- and post-adjudication processes without compromising individual rights.
- Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
- Maintaining appropriate levels of operational transparency while increasing public safety.
- Protecting the integrity of physical and behavioral health and justice system processes and information.
- Encouraging individuals to trust and cooperate with the justice system.
- Promoting governmental legitimacy and accountability.
- Making the most effective use of public resources allocated to behavioral health and public safety agencies.

The purpose of the **[name data sharing initiative]** governed by this policy is to:

- Increase the effectiveness and efficiency of the intake and classification process for **[name of entity]** providing access to treatment and supervision records across agency boundaries.
- Produce a more accurate and complete profile of offenders sentenced or assigned **[name of entity].**
- Reduce recidivism by helping to ensure that offenders—whether in a community or an incarceration setting—receive educational, vocational, rehabilitation, and/or treatment services matched to their individual needs.
- Improve continuity in services provided to offenders as they move between community supervision and incarceration.

B. Policy Applicability and Legal Compliance

1. Who is subject to the privacy policy?

Identify who must comply with the privacy policy; for example, entity personnel, participating agencies, and private contractors.

SAMPLE LANGUAGE: All **[name of entity]** personnel, participating agency personnel (including business associates and those in qualified service organizations), personnel providing information technology services to the entity, private contractors, and other authorized users will comply with the entity's privacy policy. This policy applies to medical, mental health, and substance abuse testing and treatment information the entity gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to entity personnel, treatment

providers, government agencies, and participating justice and public safety agencies (such as probation and parole), as well as to private contractors, private agencies, and the general public.

2. **How is the entity's policy made available to personnel, participating entities, and individual users (in print, online, etc.), and are acknowledgment of receipt and agreement to comply with this policy required in writing?**

   SAMPLE LANGUAGE: The **[name of entity]** will provide a printed or electronic copy of this policy to all entity and nonentity personnel who provide services and to participating agencies and individual users and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy (or applicable provisions articulated in a participating entity agreement) and the applicable provisions it contains.

3. **Does the entity require *personnel and participating information-originating and user agencies* to be in compliance with all applicable law protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of medical, mental health, and substance abuse information?**

   Cite the primary laws with which personnel and participating users must comply. This might include the U.S. Constitution and state constitutions; open records or sunshine laws; electronic health records laws; data breach notification laws; other laws, regulations, orders, opinions, or policies impacting or protecting privacy, civil rights, or civil liberties; local ordinances; and applicable federal laws and regulations, such as HIPAA, 42 CFR Part 2, etc. (For synopses of primary federal laws an agency should review for including in the privacy policy, refer to Appendix B, Listing of Applicable Federal Laws.)

   SAMPLE LANGUAGE: All **[name of entity]** personnel, participating agency personnel, personnel providing information technology services to the entity, private contractors, agencies from which medical, mental health, and substance abuse information originates, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to **[provide a list of applicable state and federal privacy, civil rights, and civil liberties laws or reference an appendix created within the entity's PHI privacy policy listing applicable federal laws]**. Through a memorandum of understanding (MOU) or a contractual agreement (business associate agreement and/or qualified service organization agreement), participating entities will acknowledge compliance with applicable provisions of this policy, which will be detailed in the MOU.

4. **Does the entity have *internal operating policies* that are in compliance with all applicable law protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of medical, mental health, and substance abuse information?**

   Cite the primary laws with which internal operating policies must be in compliance.

   SAMPLE LANGUAGE: The **[name of entity]** has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to **[provide a list of applicable state and federal privacy, civil rights, and civil liberties laws or reference to a created appendix listing such laws, including HIPAA and 42 CFR Part 2]**.

C. Governance and Oversight

1. **Who has primary responsibility for the entity's overall operation, including the entity's information systems, information collection and retention procedures, coordination of personnel, and enforcement of this policy (for example, a warden, a department of corrections administrator, director, or a state chief information officer)? Which individual will ultimately be held accountable for the operation of the information system and for any problems or errors?**

   SAMPLE LANGUAGE: Primary responsibility for the operation of the **[name of entity]**; its information systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, IQ, analysis, destruction, sharing, disclosure, or dissemination of protected health information; and the enforcement of this policy is assigned to the **[position/title]** of the entity.

2. **Does the entity have a privacy oversight committee or an individual that will develop the PHI privacy policy and/or that will routinely review and update the policy?**

SAMPLE LANGUAGE: The **[name of entity]** is guided by a designated privacy oversight committee or individual that liaises with key stakeholders (e.g., treatment providers) or entity departments and the community to ensure that privacy and civil rights are protected as provided in this policy and by the entity's protected health information-gathering and collection, retention, and dissemination processes and procedures. The committee, or individual, will annually review and update the provisions within this PHI privacy policy in response to changes in law and implementation experience, including the results of audits and inspections.

3. **Is there a designated and trained privacy officer (or privacy officer function) within the entity that will handle reported errors and violations and oversee the implementation of PHI privacy protections?**

   [Provide the title of the individual who will serve as the privacy officer, whether a full-time privacy officer position or the occupant of a different position, such as the assistant director or entity counsel. This may be a regional or partnered role as well.]

   HIPAA Note: In accordance with 45 CFR Part 164 Subpart C § 164.530(a)(1), a covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. In addition, the covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice of privacy practices required by § 164.520.

   SAMPLE LANGUAGE: The **[name of entity]**'s PHI privacy practices and policies are guided by a trained privacy officer **[who is the (position) of the entity and],** who is appointed by the **[director or other administrative title]** of the entity. The privacy officer receives reports regarding alleged errors and violations of the provisions of this PHI privacy policy and receives and coordinates complaint resolution under the entity's redress policy, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The privacy officer can be contacted at the following address**: [insert mailing address or e-mail address]**.

4. **Who is responsible for ensuring that enforcement procedures and sanctions for noncompliance with the PHI privacy policy are adequate and enforced?**

   SAMPLE LANGUAGE: The **[name of entity]**'s **[privacy officer or other position]** ensures that enforcement procedures and sanctions outlined in **[insert section number of policy (see Section N.3, Enforcement)]** are adequate and enforced.

D. Definitions

1. **What key words or phrases (and definitions) are regularly used in the policy for which the entity wants to specify particular meanings?**

   This may include terms that are not commonly known or have multiple meanings that may need to be clarified to indicate which one applies to the privacy policy. There may be legal definitions for terms in the statutes governing the operation of the information system. For examples of definitions of key terms commonly used throughout this template, refer to Appendix A, Glossary of Terms and Definitions.

   SAMPLE LANGUAGE: For examples of primary terms and definitions used in this policy, refer to **[insert section or appendix citation]**.

E. Information

1. **Identify what information *may* be sought, retained, shared, disclosed, or disseminated by the entity.**

   Note: There may be different policy provisions for different types of information, such as medical, mental health, and substance abuse testing and treatment information, as well as fact-based information databases.

   Best Practice: It is suggested that entity policies include information that details the different types of information databases/records that the entity maintains or accesses and uses.

   SAMPLE LANGUAGE: The **[name of entity]** may seek or retain the following types of information:

   - Protected health information, including medical and mental health information

- Patient identifying information, including substance abuse information
- Any information defined to be part of a designated record set—a group of records maintained by or for the entity (including medical records and billing records) about individuals that is used in whole or part by or for the entity to make decisions about individuals

- Public record information

2. Identify the purpose(s) for which information *may be* sought, retained, shared, disclosed, or disseminated by the entity.

SAMPLE LANGUAGE: The **[name of entity]** will seek or retain information that:

- Is relevant to pretrial and sentenced individuals involved in the justice system.

- Is useful in the risk, needs, and strengths analysis and in continuity of care program planning (including medical, mental health, and substance abuse treatment) for individuals involved in the justice system.

3. Identify what information *may not* be sought, retained, shared, disclosed, or redisclosed by the entity. This may include federal or state constitutional prohibitions or prohibitions in federal, state, local, or tribal law.

SAMPLE LANGUAGE: The **[name of entity]** will not seek or retain PHI (to include medical, mental health, and substance abuse testing and treatment information) **solely** on the basis of an individual's religious, political, or social views or lawful activities; his or her participation in a particular noncriminal organization or lawful event; or his or her race, ethnicity, citizenship, place of origin, gender, or sexual orientation. Such information may be sought and retained if the PHI is related to an individual's age, disability, or other medical conditions and will be received solely for purposes of providing continuity of care and treatment and/or verifying compliance with court-ordered substance abuse or behavioral health program participation.

4. When PHI is gathered or collected and retained by the entity (or received from an information providing entity), are limitations assigned to identify who is allowed to see (access) and use the information (for example, credentialed, role-based levels of access) and is the PHI labeled (by record, data set, or system of records) to indicate to the authorized information recipient that:

- **The information is protected health information, including personally identifiable information on any individual regardless of citizenship or U.S. residency status?**
- **The information is subject to specific health information privacy or other similar restrictions on access, use, disclosure, or redisclosure and, if so, what is the nature of such restrictions?**

There may be laws that restrict who can access information, how information can be used, and the retention or disclosure of certain types of information.

HIPAA/42 CFR Part 2 Notes:

a. In accordance with 45 CFR Part 164 Subpart E § 164.514(d)(2)(i), a HIPAA-covered entity must identify those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties and for each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

b. In accordance with 42 CFR Part 2 Subpart B § 2.12(c)(3), communication of information within the program (or to an entity with direct administrative control over the program) is to be limited to those persons who have a need for the information in connection with their duties that arise out of the provision of diagnosis, treatment, or referral for treatment of substance abuse.

SAMPLE LANGUAGE: The **[name of entity]** applies labels (by record, data set, or system of records), to the maximum extent feasible, to entity-originated PHI (or ensures that the PHI-providing entity has applied labels) to indicate to the accessing authorized information recipient that:

- The information is "protected health information" (see Terms and Definitions, within this policy) subject to **[local, state, or federal]** laws restricting access, use, disclosure, or redisclosure, including 45 CFR Part 164 § 164.514 (HIPAA for medical and mental health information) and 42 CFR Part 2 Subpart B § 2.12(c)(3) (for substance abuse information).

- The information has applicable limitations on access and sensitivity of disclosure, as such the information is labeled to:
    - Protect an individual's right of privacy or his or her civil rights and civil liberties.
    - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, or resident of a mental health treatment program.

5. **Does your entity categorize information (or ensure that the PHI-providing entity has categorized information) based on its nature (for example, conditions of supervision, medical, mental health, and substance abuse testing and treatment information), usability, and quality?**

   The purpose of categorizing information is to assist information recipients in:

   - **Determining the quality and accuracy of the information.**
   - **Making the most effective use of the information.**
   - **Knowing whether and with whom the information can be appropriately shared.**

   SAMPLE LANGUAGE: The **[name of entity]** personnel will, upon receipt of PHI, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to PHI (or ensure that the PHI-providing entity has assigned categories to the information), as appropriate, to reflect the assessment, such as:

   - Whether the information consists of conditions of supervision, medical, mental health, substance abuse testing or treatment information, or other information category.
   - The nature of the source (for example, physician, counselor).
   - The validity of the information provided (for example, self-reported, verified by intake/classification personnel, excerpted from clinical record or case notes).

6. **What conditions prompt the labels assigned in E.4. and E.5. to be reevaluated?**

   SAMPLE LANGUAGE: The labels assigned to existing information under [**insert section number of PHI policy**] will be reevaluated whenever:

   - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
   - There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7. **Does your entity require certain basic descriptive information (metadata tags or labels) to be entered and associated with each record, data set, or system of records containing PHI that will be accessed, used, and disclosed?**

   SAMPLE LANGUAGE: The **[name of entity]** requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure. The types of information include:

   - The name of the PHI-providing entity (if self-reported), and the entity's department, component, or subcomponent (if applicable).
   - The name of the entity's information system from which the information is disseminated.
   - The date the information was collected and, when feasible, the date its accuracy was last verified.

- The title and contact information for the person to whom questions regarding the information should be directed.

8. Does your entity maintain a record of the source of the information sought and collected?

SAMPLE LANGUAGE: The **[name of entity]** will keep a record of the source of all information sought and collected by the entity, including the date the information was received.

F. Acquiring and Receiving Information

1. Do agencies that access your entity's PHI and/or share PHI with your entity ensure that they will adhere to applicable laws and policies?

SAMPLE LANGUAGE: External agencies that access the **[name of entity]**'s PHI or share PHI with the entity will provide an assurance (e.g., within interagency agreements, MOUs) that they comply with law governing those individual entities, including applicable federal and state laws.

2. If the entity contracts with commercial databases, how does the entity ensure that the commercial database company is in legal compliance in its information-gathering techniques?

SAMPLE LANGUAGE: The **[name of entity]** will contract only with commercial database companies that provide an assurance that their methods for gathering PHI comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

G. Information Quality Assurance

1. Does your entity have established protocols and procedures (manual and electronic) to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the PHI it collects, maintains, and disseminates?

SAMPLE LANGUAGE: The **[name of entity]** will make every reasonable effort to ensure that the PHI sought or retained is derived from dependable and trustworthy sources; sufficiently accurate; current; and complete, considering the relevant context in which it was sought or received and the purpose for which it will be used.

2. Does your entity research alleged or suspected errors and deficiencies (or refer them to the PHI-providing agency)? How does your entity respond to confirmed errors or deficiencies?

SAMPLE LANGUAGE: The **[name of entity]** investigates, in a timely manner, alleged errors and deficiencies (or refers them to the PHI-providing agency) and corrects, flags, amends, deletes, or refrains from using PHI found to be erroneous or deficient.

3. When the entity reviews the quality of the PHI it originates and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, <u>what is the entity's procedure for correction or destruction</u>?

SAMPLE LANGUAGE: The **[name of entity]** will conduct periodic data quality reviews of PHI it originates and make every reasonable effort to ensure that the PHI will be corrected, flagged or amended in the system, deleted, or not used when the entity identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; or the entity erroneously received PHI or provided PHI to another agency.

4. When the entity reviews the quality of the PHI <u>it has received from</u> an originating agency and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, <u>does the entity notify the originating agency</u> or the originating agency's privacy officer? What method is used to notify the agency (written, telephone, or electronic notification)?

SAMPLE LANGUAGE: Originating agencies external to the **[name of entity]** are responsible for reviewing the quality and accuracy of the PHI provided to the entity. The entity will review the quality of PHI it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

5. **When the entity reviews the quality of the PHI it has provided to an external agency and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, does the entity notify the external agency? What method is used to notify the agency (written, telephone, or electronic notification)?**

   SAMPLE LANGUAGE: The **[name of entity]** will use written or electronic notification to inform recipient agencies when PHI previously provided to the recipient agency is deleted or changed by the entity because the PHI is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

6. **For covered entities, when the entity is informed by another covered entity of an amendment to an individual's PHI, what is the entity's procedure for amendment?**

   HIPAA Note: In accordance with 45 CFR Part 164 Subpart C § 164.526(e), a covered entity that is informed by another covered entity of an amendment to an individual's PHI must amend the PHI.

   SAMPLE LANGUAGE: The **[name of entity]**, if notified by another covered entity of an amendment to an individual's PHI, will amend the PHI in the designated record set that is maintained by the entity.

H. Program Evaluation and Research

In the following HIPAA and 42 CFR Part 2 requirements for research, entities can share deidentified information, as well as the results of analysis which has also been deidentified.

HIPAA/42 CFR Part 2 Notes:

a. **In accordance with 45 CFR Part 164 Subpart C § 164.502(d) and § 164.514, HIPAA-covered entities may use PHI to create information that is not PHI or disclose PHI only to a business associate for such purpose, whether or not the deidentified information is to be used by the covered entity. (See Appendix A, for a definition of business associate.) Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not considered to be PHI, (i.e., it is deidentified). (Refer to § 164.502(d) for uses and disclosures of deidentified information and § 164.514 for requirements for deidentified information.)**

b. **In accordance with 42 CFR Part 2 Subpart B § 2.11 and 2.12(a), programs are permitted to disclose information about a patient if the disclosure does not identify the patient as a substance abuser or as someone who has applied for or received substance abuse assessment or treatment services.**

c. **In accordance with 42 CFR Part 2 Subpart D § 2.52, patient identifying information may be disclosed for the purpose of conducting scientific research if the program director makes a determination that the recipient of the patient identifying information is qualified to conduct the research; has a research protocol under which the information will be maintained in accordance with the security requirements of § 2.16; and will not be redisclosed except back to the program from which that information was obtained and may not identify any individual patient in any report of that research or otherwise disclose patient identities; and has provided a satisfactory written statement that a group of three or more individuals who are independent of the research project has reviewed the protocol and determined that the rights and welfare of patients will be adequately protected and the risks in disclosing patient identifying information are outweighed by the potential benefits of the research.**

1. **Who is authorized (position/title, credentials, etc.) to analyze deidentified PHI for evaluation and research purposes?**

   SAMPLE LANGUAGE: Only PHI that has been deidentified such that it does not and cannot be used to identify an individual will be analyzed, for evaluation and research purposes, only by qualified individuals who have been selected, approved, and trained accordingly and who are authorized by state and federal law.

2. **What information is analyzed?**

   SAMPLE LANGUAGE: Only PHI that is deidentified such that it does not and cannot be used to identify an individual will be subject to collation and analysis.

3. **For what purpose(s) is deidentified PHI analyzed?**

   SAMPLE LANGUAGE: PHI that is deidentified such that it does not and cannot be used to identify an individual will be analyzed only for evaluation and research purposes.

I. Merging Records

1. **Who is authorized (position/title, credentials, etc.) to merge records?**

   SAMPLE LANGUAGE: PHI from multiple records allegedly about the same individual will be merged only by qualified individuals who have successfully completed a background check, if applicable, and have been selected, approved, and trained accordingly.

2. **What matching criteria does your entity require when attempting to merge PHI from multiple records allegedly about the same individual? In other words, when two records are compared for possible merger, are there certain attributes (name, date of birth, social security number, etc.) that must match, or is there a minimum number of attributes (for example, two out of five) that must match to link the two records as relating to the same person?**

   SAMPLE LANGUAGE: PHI records about an individual from two or more sources will not be merged by the **[name of entity]** unless there is sufficient identifying information to clearly establish that the PHI is about the same individual. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match.

3. **If the criteria specified in Section I.2 are not met, does the entity have a procedure for associating PHI records?**

   SAMPLE LANGUAGE: If the matching requirements are not fully met but there is reason to believe the PHI records may be about the same individual, the PHI may be "associated" by the **[name of entity]** if accompanied by a clear statement that it has not been adequately established that the PHI relates to the same individual.

J. Use and Disclosure

1. **What types of information recipient actions and permissions are controlled by the entity's access or dissemination limitations?**

   Information recipient actions and permissions are often used to identify entities and individuals with a need and right to know particular information; to access case management information (including medical, mental health, and/or substance abuse); access nonpersonally identifiable information only; or to identify who is authorized to submit or modify particular records or record sets, to have read-only access or to be authorized to add/modify/delete records, or to be authorized to grant privileges.

   <u>HIPAA/42 CFR Part 2 Notes</u>:

   a. **In accordance with 45 CFR Part 164 Subpart E § 164.514(d)(2)(i), a HIPAA-covered entity must identify those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties and for each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.**

   b. **In accordance with 42 CFR Part 2 Subpart B § 2.12(c)(3), communication of information within the program (or to an entity with direct administrative control over the program) should be limited to those persons who have a need for the information in connection with their duties that arise out of the provision of diagnosis, treatment or referral for treatment of substance abuse.**

   <u>Best Practice</u>: It is suggested that entities specify their methods for identifying information recipient actions and permissions in their privacy policies.

SAMPLE LANGUAGE: Credentialed, role-based access criteria will be used by the **[name of entity]**, as appropriate, to control:

- The information to which a particular group or class of information recipients can have access based on the group or class.

- The information a class of information recipients can add, change, delete, or print.
- To whom, individually, the information can be disclosed and under what circumstances.

2. What limitations has the entity implemented to limit or restrict disclosure of PHI?

HIPAA/42 CFR Part 2 Notes:

a. In accordance with 45 CFR Part 164 Subpart C § 164.514 (d) Standard minimum necessary requirements, (3)(i) and (ii), for any PHI disclosures made by the HIPAA-covered entity on a routine and recurring basis, the covered entity must implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. (ii) For all other disclosures, the covered entity must develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought and review requests for PHI on an individual basis in accordance with such criteria.

b. In accordance with 42 CFR Part 2 Subpart B § 2.13, any disclosure [whether authorized by patient consent or per exceptions cited in § 2.12(c)] made under these regulations must be limited to that information which is necessary to carry out the purpose of the disclosure.

c. In accordance with 42 CFR Part 2 Subpart B § 2.13(c)(2), any answer to a request for a disclosure of patient records which is not permissible under these regulations must be made in a way that will not affirmatively reveal that an identified individual has been, or is being diagnosed or treated for substance abuse. An inquiring party may be given a copy of these regulations and advised that they restrict the disclosure of substance abuse patient records, but may not be told affirmatively that the regulations restrict the disclosure of the records of an identified patient. The regulations do not, however, restrict a disclosure that an identified individual is not and never has been a patient.

SAMPLE LANGUAGE: The **[name of entity]**, for any PHI disclosures that are made on a routine and recurring basis, will follow implemented policies and procedures that limit the amount of information disclosed to that which is reasonably necessary, in accordance with established criteria, in order to achieve the purpose of the disclosure, such as to provide treatment. For other disclosures, the entity will review requests for PHI on an individual basis and in compliance with such entity-established criteria. For requests for disclosure of patient records which are not permissible, the entity will respond to the request in such a way that will not affirmatively reveal that an identified individual has been or is being diagnosed or treated for substance abuse or any other condition.

3. Describe the conditions and credentials by which access to and disclosure of PHI records retained by the entity will be provided *within the entity or in other governmental agencies*. Is an audit trail kept of access to and disclosure of PHI retained by the entity (e.g., dissemination logs)?

HIPAA Notes:

a. In accordance with 45 CFR Part 164 Subpart C § 164.506, HIPAA-covered entities may use or disclose PHI for its own treatment, payment, or health-care operations without requiring individual authorization, except for disclosures described in § 164.508 (see J.4. below).

b. In accordance with 45 CFR Part 164 § 164.512(k)(5), HIPAA-covered entities are permitted to disclose PHI without the written authorization of the individual or the opportunity for the individual to agree or object for specialized government functions, such as to a correctional institution or other law enforcement official having lawful custody of an inmate or other individual when the PHI is about such inmate or individual and if the correctional institution or such law enforcement official represents that such PHI is necessary for:

- **The provision of health care to such individuals;**

- **The health and safety of such individual or other inmates;**

- **The health and safety of the officers or employees of or others at the correctional institution;**

- **The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;**

- **Law enforcement on the premises of the correctional institution; or**
- **The administration and maintenance of the safety, security, and good order of the correctional institution.**

SAMPLE LANGUAGE: Access to or disclosure of PHI retained by the **[name of entity]** will be provided only ***to persons within the entity*** who are authorized to have access and only for diagnosis, treatment, or referral for treatment, payment, or health care operations purposes or for the health and safety of the individual, other inmates, officers or employees of the institution responsible for transporting inmates, or the administration and maintenance of the safety, security, and good order of the **[name of entity]**. An audit trail sufficient to allow the identification of each individual who accesses information retained by the entity and the nature of the information accessed will be kept by the entity.

4. **Describe the conditions by which access to and disclosure of PHI retained by the entity are <u>not permitted without an individual consent authorization</u>.**

   <u>HIPAA Notes</u>:

   a. **In accordance with 45 CFR Part 164 Subpart C § 164.512(k)(5)(iii), individuals who are <u>no longer in lawful custody</u> of a correctional institution or other law enforcement facility, must provide a consent authorization in order for the [name of entity] to disclose PHI.**

   b. **In accordance with 45 CFR Part 164 Subpart C § 164.508, a HIPAA-covered entity may not use or disclose PHI without an authorization for any use of**

      - **psychotherapy notes, except for:**

        - **use by the originator of the notes for treatment,**

        - **use or disclosure by the covered entity for its own training programs in which students, trainees or practitioners in mental health learn under supervisions to practice of improve their skills in group, joint, family, or individual counseling; or**

        - **use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual.**

   SAMPLE LANGUAGE: The **[name of entity]** will not use or disclose PHI without a valid individual consent authorization if the individual to whom the PHI pertains is no longer in lawful custody, as per 45 CFR Part 164 Subpart C § 164.512(k)(5)(iii).

   The **[name of entity]** will not use or disclose PHI without a valid individual consent authorization (that meets the core element requirements for authorizations per 45 CFR Part 164 Subpart C § 164.508(c)), (excepting psychotherapy notes cited in 45 CFR Part 164 Subpart C § 164.508(a)(2)), and 42 CFR Part 2 § 2.31. An individual, however, may revoke an authorization at any time, per 45 CFR Part 164 Subpart C § 164.508(b)(5) and per 42 CFR Part 2 § 2.31, provided that the revocation is in writing, except to the extent that the covered entity has taken action in reliance thereon; or if the authorization was obtained as a condition of obtaining insurance coverage.

   The entity will document and retain any signed consent authorization and will provide the individual with a copy of the signed authorization.

5. **Does the entity permit released individuals (those who are no longer in lawful custody) to restrict the use and disclosure of the PHI that is about the individual?**

   <u>HIPAA Note</u>: In accordance with 45 CFR Part 164 Subpart C § 164.522 (a)(1), a covered entity <u>must</u> permit an individual to request that the covered entity restrict uses or disclosures of PHI about the individual to carry out treatment, payment, or health-care operations and disclosures permitted under § 164.510(b). A

covered entity, however, is not required to agree to a restriction. If, however, the entity agrees to the restriction it is required to follow the conditions and procedures described in § 164.522 (a)(1).

SAMPLE LANGUAGE: The **[name of entity]** will permit released individuals (those who are no longer in lawful custody) to request that the entity restrict use or disclosure of the individuals' PHI retained by the entity. If the entity agrees to the restriction, the entity will follow the conditions and procedures cited in 45 CFR Part 164 Subpart C § 164.522, regarding rights to request privacy protection for PHI.

6. **For individuals who are released from custody (for example, on probation or parole), what are the conditions by which the entity may use or disclose PHI without the individuals' written consent authorization?**

   SAMPLE LANGUAGE: The [name of entity] may use or disclose PHI about an individual who is released from incarceration and no longer in lawful custody without requiring a written consent authorization for the following conditions:

   - Uses and disclosures required by law
   - Uses and disclosures for public health activities
   - Mandatory reports to law enforcement of suspected crimes (e.g., domestic violence, child abuse, neglect)
   - Uses and disclosures for health oversight activities
   - Disclosures for judicial, administrative, and investigative proceedings
   - Disclosures for law enforcement purposes
   - Uses and disclosures about decedents, where applicable
   - Uses and disclosures of deidentified information for research purposes
   - Uses or disclosures to avert a serious threat to health or safety
   - Uses for specialized government functions, including for military purposes
   - Disclosures for workers' compensation, if applicable

7. **Are participating agencies that access information from your entity required to obtain approval from the originator of the information prior to further dissemination or to follow the disclosure or redisclosure law applicable to the originating agency?**

   <u>42 CFR Part 2 Notes</u>:

   a. **In accordance with 42 CFR Part 2 Subpart C § 2.32, if 42 CFR Part 2 information has been disclosed to an outside provider agency, either pursuant to a 42 CFR Part 2-compliant written consent form authorizing such disclosure or under a Qualified Service Organization Agreement (QSOA), the outside agency may disclose 42 CFR Part 2 information that it has received to affiliated outside agencies ONLY if the patient signs a 42 CFR Part-2 compliant consent form authorizing such third-party dissemination.**

   b. **Also, under 42 CFR Part 2, a single consent form can authorize a disclosure of information about a patient to one or more recipients, and simultaneously authorize that recipient to redisclose that information to any additional entity or entities (such as other affiliated health-care providers identified in the consent form), provided that the purpose for the disclosure is the same. The following required statement prohibiting redisclosure must accompany the information disclosed through consent, so that each subsequent recipient of that information is notified of the prohibitions on redisclosure.**

      This notice covers the disclosure of information to you concerning a client in alcohol/drug treatment, made to you with the consent of such client. This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR Part 2). The federal rules prohibit you

> ***from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any substance abuse patient.***

c. In accordance with 42 CFR Part 2 Subpart B § 2.13(a) and in contrast to circumstances where information is disclosed through patient consent, if a medical emergency exists 42 CFR Part 2 provisions do not prohibit the redisclosure of 42 CFR Part 2 information once it is released. Consequently, medical personnel treating a patient for a medical emergency who are affiliated providers may download and include in their own records the information they obtained in treating the emergency, and may then redisclose that information to others without obtaining patient consent. However, all disclosures of information under the regulation must be limited to the information necessary to carry out the purpose of the disclosure.

SAMPLE LANGUAGE: Agencies external to the **[name of entity]** may not disseminate information accessed or disseminated from the entity without approval from the entity or other originator of the information or, if subject to 42 CFR Part 2 (for substance abuse information), consent of the individual to whom the information pertains, or as otherwise authorized by law. Redisclosure of 42 CFR Part 2 information will be made only in accordance with written individual consent or as part of a Qualified Service Organization Agreement (QSOA). The following notice will accompany any such disclosures of 42 CFR Part 2 information.

> *This notice covers the disclosure of information to you concerning a client in alcohol/drug treatment, made to you with the consent of such client. This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any substance abuse patient.*

8. Describe the conditions under which access to and disclosure of PHI records retained by the entity will be provided *to those responsible for medical, mental health and/or behavioral health, including substance abuse services*. Is an audit trail kept of access to and disclosure of information retained by the entity (e.g., dissemination logs)?

<u>HIPAA Note</u>: In accordance with 45 CFR Part 164 Subpart C § 164.506, HIPAA-covered entities may use or disclose PHI: for its own treatment, payment, or health-care operations; for treatment activities of a health-care provider; to another covered entity or health-care provider for the payment activities of the entity that receives the information; or to another covered entity for health-care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure meets the definition of "health care operations" (see definition in Appendix A of "Health Care Operations.").

SAMPLE LANGUAGE: PHI records retained by the **[name of entity]** may be accessed by or disseminated ***to providers responsible for medical, mental health, and/or behavioral health, including substance abuse services*** only for offender treatment and continuity of care purposes as authorized by law and only in the performance of official duties in accordance with applicable law and procedures. An audit trail sufficient to allow the identification of each organization and individual who accessed or received information retained by the entity, the date, and the nature of the information accessed will be kept by the entity.

9. Under what circumstances and what legal authority will access to and disclosure of a record be provided *to a member of the public* in response to an information request, and are these circumstances described in your entity's redress policy? Is an audit trail kept of access to and disclosure of information retained by the entity without the audit trail constituting an impermissible collection of information of a member of the public (e.g., dissemination logs)?

Note: This issue does not apply to circumstances in which an entity chooses to provide nonsensitive information to the public or to provide sensitive information in accordance with entity policy in response to an emergency situation.

SAMPLE LANGUAGE: Information gathered or collected and records retained by the **[name of entity]** may be accessed or disclosed ***to a member of the public*** only if the information is defined by law **[cite applicable law]** to be a public record or if the record is PHI that is permitted to be accessible in accordance with HIPAA and 42 CFR Part 2 and with the conditions cited in K.1 Disclosure of this privacy policy, or is otherwise appropriate for release and is not exempt from disclosure by law. The **[name of entity]**, however, may disclose records relating to the management and direction of a law enforcement agency and records reflecting the initial arrest of an adult and the charge or charges brought against an adult, if applicable by law [**insert state citation**]. In addition, the following information regarding inmates/offenders may be made available to a member of the public in accordance with [**insert state law citation**]:

- Inmate/offender's name
- Inmate/offender's age (but not date of birth)
- Inmate/offender's last known city or town of residence (but not street address)
- Record of incarceration, to include any/all information concerning dates of incarceration (present and prior)
- Court of jurisdiction
- Parole eligibility date
- Probation dates
- Assigned facility (if currently incarcerated)
- Discipline status and number of previous disciplines
- Community confinement dates

Such information may be disclosed only in accordance with the law and procedures applicable to the entity for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the entity, the date, and the nature of the information accessed will be kept by the entity but may be disclosed only in connection to a challenge to the legitimacy of the disclosure itself but not for investigatory or other criminal justice purposes.

10. **If release of information can be made only under specific conditions (for specific purposes or to specific persons), are those conditions described? Is an audit trail kept showing how those conditions were met?**

    Refer to N.2, Accountability, for more information on audit logs.

    SAMPLE LANGUAGE: PHI gathered or collected and records retained by the **[name of entity]** may be accessed or disseminated ***for specific purposes*** upon request by persons authorized by law to have such access and only for those uses and purposes specified in the federal or state law. This includes medical emergencies under 42 CFR Part 2 Subpart C § 2.51, provided that patient notification is provided immediately following disclosure. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the entity; the date; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of [**specify the retention period for your jurisdiction for this type of request**] by the entity.

11. **Under what circumstances and to whom will the entity *not disclose* PHI records?**

    SAMPLE LANGUAGE: PHI gathered or collected and records retained by the **[name of entity] will not** be

    - Sold, published, exchanged, disclosed, or redisclosed for commercial purposes.

- Disclosed, redisclosed, or published without prior notice to the information-providing entity that such information is subject to disclosure or publication, unless disclosure or redisclosure is authorized by law and is agreed to as part of the normal operations of the entity.

- Disclosed or redisclosed to persons not authorized to access or use the information.

- Disclosed or redisclosed, if it is substance abuse information, without the consent of the patient, except in the case of a medical emergency or court order.
- Disclosed or redisclosed, if it is medical or mental health information of a ***former*** inmate without a written consent authorization provided by the patient, except in the case of preventing or lessening a serious and imminent threat or safety of a person or the public or in response to a court order, subpoena, or other lawful process.

12. What are the categories of records that ordinarily will *not be provided* to the public pursuant to applicable legal authority [the policy must cite applicable legal authority for each stated category]?

SAMPLE LANGUAGE: There are several categories of records that ordinarily will not be provided to the public:

- Records required to be kept confidential by law are exempted from disclosure requirements under **[cite public records act and applicable section]**.

- Records relating to a client/attorney relationship **[cite applicable law]**.

- Information relating to inmates/offenders that may pose a risk to the facility or public safety **[cite applicable law]**.

- Information relating to inmates/offenders that contains the opinions and/or recommendations of members of established facility boards and/or committees (including, but not limited to classification and disciplinary boards) and/or may compromise the personal or official discretion of any member **[cite applicable law]**.

- Information relating to inmates/offenders that contains medical/psychological test results, reports, and/or information **[cite applicable law]**.

- Security classification of individuals **[cite applicable law]**.

- Medical and mental health records as protected by HIPAA.

- Substance abuse testing and treatment records as protected by 42 CFR Part 2.

- Protected federal, state, local, or tribal records, which may include records originated and controlled by another entity that cannot, under **[cite applicable law]**, be shared without permission.

- A violation of an authorized nondisclosure agreement under **[cite applicable law]**.

13. State the entity's policy on confirming the existence or nonexistence of information to persons or agencies that are not eligible to receive the information.

SAMPLE LANGUAGE: The **[name of entity]** shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law.

K. Redress

K.1 Disclosure

1. If required by state statute or federal law, what are the conditions under which the entity will disclose PHI contained in the entity's designated record set to an individual about whom the information was gathered? Is a record kept of all requests and of what information is disclosed to an individual?

Note: If the state public (open) records act provides procedures for disclosure, corrections, appeals, and handling of complaints when information is not subject to disclosure, these procedures should be summarized in the privacy policy in lieu of using the sample language for that type of information.

HIPAA/42 CFR Part 2 Notes:

a. **In accordance with 45 CFR Part 164 Subpart C § 164.524 and section § 13405(e) of the HITECH Act, an individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set for as long as the PHI is maintained in the designated record set, except for:**

- **psychotherapy notes,**
- **information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and**

- **the PHI maintained by the entity is subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law or exempt pursuant to 42 CFR 493.3(a)(2).**[24]

A designated record set includes: (1) a health-care provider's medical and billing records, (2) a health plan's enrollment, payment, claims adjudication, and case or medical management records systems, and (3) any information used, in whole or in part, by or for the covered entity to make decisions about individuals. A record is any item (whether in paper or electronic format), collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the covered entity, per 45 CFR § 164.501.

b. **In accordance with 45 CFR Part 164 Subpart C § 164.524(b)(2)(i) and (ii), covered entities must act on a request for access no later than 30 days after receipt of the** request. If the request for access is for PHI that is NOT maintained or accessible to the covered entity on-site, the entity must take action by no later than 60 days from the receipt of such a request.

c. **In accordance with 45 CFR Part 164 Subpart C § 164.524(c)(2)(i) and (ii), covered entities must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual. The covered entity is required to provide electronic information to an individual in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. If the individual declines to accept any of the electronic formats that are readily producible by the covered entity, the covered entity must provide a hard copy as an option to fulfill the access request.**

d. **In accordance with 45 CFR part 164 Subpart C § 164.524(b)(2)(iii), if the covered entity is unable to take an action required by (b)(2)(i) and (ii) within the time required by paragraph, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that the covered entity, within the time limit set by (b)(2)(i) [30 days for on-site PHI] or (b)(2)(ii) [60 days, for PHI not maintained or accessible on-site] as applicable, and provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request. The covered entity may have only one such extension of time for action on a request for access.**

e. **In accordance with 45 CFR Part 164 Subpart C § 164.510(b)(5), HIPAA-covered entities are permitted to disclose a decedent's PHI, in addition to the individual's personal representative, to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.**

f. **In accordance with 42 CFR Part 2 Subpart B § 2.23, patients may have access to his or her own records, including the opportunity to inspect and copy any records that the program maintains about the patient. The program is not required to obtain a patient's written consent or other authorization in order to provide such access to the patient. Information obtained by patient access to his or her patient record is subject to the restriction on use of his information to initiate**

[24] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf

or substantiate any criminal charges against the patient or to conduct any criminal investigation of the patient as provided for under § 2.12(d)(1).

SAMPLE LANGUAGE: If required by state statute or federal law (such as 45 CFR § 164.514(h)(1)) for medical and mental health information, or 42 CFR Part 2 Subpart B § 2.23 for substance abuse treatment information), and upon satisfactory verification (driver's license, state identification card, or other specified identifying documentation) of his or her identity and subject to the conditions specified in K.1, 2., below, an individual is entitled to know the existence of and to review the information contained in the entity's designated record set about him or her that has been gathered and retained by the **[name of entity]**. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information (correction). The entity will provide a copy of the PHI contained in the designated record set to the individual in the form or format request by the individual, if it is readily producible in such form or format, or, if not, in a readable hard-copy form or such other form or format as agreed to by the entity and the individual. If the individual requests that the information be provided in electronic format, the [**name of entity**] will provide the information to the individual in the electronic form or format agreed to by the individual and the [**name of entity**]. If the individual declines to accept any of the electronic formats that are readily producible by the [**name of entity**], the [**name of entity**] will provide a hard copy as an option to fulfill the access request.

A personal (i.e., legal) representative, family member, or other individual involved in the care or payment for care of a decedent prior to death is entitled to know the existence of and to review the information about the decedent that has been gathered and retained by the **[name of entity]**.

The entity will respond to the request for access to PHI (in writing or electronically) within 30 days for PHI that is maintained and accessible on-site and within 60 days for PHI that is NOT maintained or accessible to the entity on-site, per 45 CFR § 164.524(b)(2)(i) and (ii), and in a form that is readily intelligible to the individual. If the entity is unable to grant access within the time limits specified by 45 CFR § 164.524(b)(2)(i) and (ii), the entity may extend the time for such actions by no more than 30 days and will provide the individual with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request. A record will be kept of all requests and of what information is disclosed to an individual.

2. **If requested by an individual, what are the conditions under which the covered entity will transmit a copy of the individual's PHI from the entity's designated record set to a third-party person designated by the individual?**

   HIPAA Note:

   a. **In accordance with 45 CFR Part 164 Subpart C § 164.524(c)(3) and in compliance with the HITECH Act, § 13405(e)(1), if requested by an individual, a covered entity must transmit the copy of PHI directly to a person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of PHI. The covered entity may employ an electronic process for receiving an individual's request to transmit a copy of PHI to his or her designee. Whether the process is electronic or paper-based, a covered entity must implement reasonable policies and procedures under § 164.514(h) to verify the identity of any person who requests PHI, as well as implement reasonable safeguards under § 164.530(c) to protect the information that is used or disclosed.**

   If requested by an individual, the [**name of entity**] will transmit a copy of an individual's PHI, from the entity's designated record set, directly to a person designated by the individual. The individual's request must be in writing, be signed by the individual, and clearly identify the designated person and where to send the copy of PHI. The [**name of entity**] will follow policies and procedures (refer to K.1, 1.) to verify the identity of the person who requests PHI and implement reasonable safeguards to protect the information that is used or disclosed in accordance with section L. Information Security Safeguards.

3. **What are the conditions under which the entity will not disclose information to an individual about whom information has been gathered? Does the entity refer the individual to the agency originating the information?**

   HIPAA Notes:

a. In accordance with 45 CFR Part 164 Subpart C § 164.524(b)(2)(iii), if the entity is unable to take action to a request for PHI, the entity may extend the time for such actions by no more than 30 days provided that the entity provides the individual with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request and the entity may have only one such extension.

b. In accordance with 45 CFR Part 164 Subpart C § 164.524(d)(3), if the covered entity does not maintain the PHI that is the subject of the individual's request for access and the entity knows where the requested information is maintained, the entity must inform the individual where to direct the request for access.

Note: It is up to the entity to determine which process to use for referrals, whether the entity will refer an individual to the provider or whether the entity will contact the provider and inform them of the individual's request, or both.
SAMPLE LANGUAGE: The existence, content, and source of the information will not be made available by the **[name of entity]** to an individual when the following conditions exist. **[Note: The policy must cite applicable legal authority for each stated basis for denial.]**

- The information is PHI but access is being requested by a person who is not legally authorized to act on behalf of the individual to whom the PHI applies, per 45 CFR § 164.502(g)(1).
- The information is PHI that meets the access denial conditions cited in 45 CFR § 164.524(a)(2) and (3), such as psychotherapy notes (1996 Supreme Court ruling, Jaffee v. Redmond, 518 U.S. 1.).
- The information was part of a disclosure of PHI made to correctional institutions or law enforcement officials, as provided in 45 CFR § 164.512(k)(5).
- The information source does not reside with the entity.
- The entity did not originate and does not have a right to disclose the information.
- The information is:
    - Administrative data, which is patient-identifiable and used for administrative, regulatory, or other health care operations, such as event history/audit trails, data used for quality assurance or utilization management, data prepared in anticipation of legal action, etc.
    - Derived data stored in aggregate or summarized which is not patient-identifiable, such as data used for accreditation reports, research data, statistical reports, best practice guidelines, etc.
    - Psychotherapy notes maintained separate from the rest of the patient's medical record.
    - Patient information created as part of a research study to which the patient has temporarily waived right to access.
    - Records that have been destroyed because they have exceeded their required retention period or because they have been rendered unusable due to fire, flood, or other circumstances.
    - Subject to a legal privilege such as peer review or attorney/client privilege.
- Other **authorized** basis for denial.

If the information does not originate with the entity (e.g., the entity received or accesses the information from another source), the requestor will be referred to the provider agency, if appropriate or required, **or** the entity will notify the source agency of the request and its determination that disclosure **by the entity** or referral **of the requestor** to the source agency was neither required nor appropriate under applicable law.

K.2 Data Amendments

1. For HIPAA-covered entities, does your institution have a point of contact for handling individuals' requests for amendments of PHI in the designated record set, and does the entity retain documentation of the title(s) of the person(s) or office(s) responsible?

HIPAA Note: In accordance with 45 CFR Part 164 Subpart C § 164.526(f), a covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments of PHI by individuals and retain the documentation in accordance with § 164.530(j).

SAMPLE LANGUAGE: The **[name of entity]**'s **[privacy officer or state other position title or office]** will be responsible for receiving and processing requests for amendments (corrections) by individuals to PHI contained in the entity's designated record set. The **[name of entity]** will maintain a record of the titles of the persons or offices responsible for handling such requests.

2. What is the entity's procedure for handling individuals' requests for correction (or amendments) involving *information in a designated record set that the entity can change because it originated the information*? Is a record kept of requests for corrections (amendments)?

HIPAA Notes:

a. Right to amend: In accordance with 45 CFR Part 164 Subpart C § 164.526, an individual has the right to have a covered entity amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set in a manner that is fully consistent with the Correction Principle in the Privacy and Security Framework, and the HIPAA Right to Amend 45 CFR § 164.526(a).

b. Time period: In accordance with 45 CFR Part 164 Subpart C § 164.526(b)(2)(i) and (ii), the covered entity must act on the individual's request for amendment no later than 60 days after receipt of such request. If the entity is unable to act on the amendment within the time required, the covered entity may extend the time for such action by no more than 30 days provided the entity, within the time limit, provides the individual with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request and the entity may have only one such extension of time.

c. Request for amendment granted: In accordance with 45 CFR Part 164 Subpart C § 164.526(c), if the covered entity grants the request, the entity must make the appropriate amendment to the PHI or record by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment and will timely inform the individual that the amendment is accepted and obtain the individual's identification of and an agreement to have the entity notify the relevant persons with which the amendment needs to be shared. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the individual as having received the PHI and person, including business associates, that the entity knows has the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

d. Request for amendment denied: In accordance with 45 CFR Part 164 Subpart C § 164.526(b)(2)(i)(B) and (d), if the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a timely written denial, in plain language, which contains:

- **The basis for the denial,**
- **The individual's right to submit a written statement of disagreement with the denial and how the individual may file such a statement,**
- **A statement that, if the individual does not submit a statement of disagreement, the individual may request that the entity provide the individual's request for amendment and the denial with any future disclosures of the PHI, and**
- **A description of how the individual may complain to the entity, including the name, or title, and telephone number of the contact person or office.**

SAMPLE LANGUAGE: If an individual requests correction of PHI contained in the entity's designated record set, *originating with the **[name of entity],*** the entity's privacy officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. The entity will act in a timely manner, within 60 days, to amend the

record as requested by the individual, and to notify the individual of the entity's acceptance to amend the record, or to notify the individual that the request is denied. When a record is amended, the entity will make every reasonable effort to ensure that the amended information is provided to participating agencies, health information organizations, and others who are known to have received the PHI. When the request is denied, the entity will notify the individual in writing of the basis for denial, his or her right and the procedure for submitting a written statement of disagreement, the option for the individual to request, in lieu of a statement of disagreement, that the entity provide both the individual's request for amendment and the entity's denial with any future disclosures of the PHI, and entity contact information for submitting the complaint. A record will be kept of all requests for corrections and amendments and the resulting action, if any.

K.3 Appeals

1. What are the conditions under which the entity may deny an individual's request for access or correction (amendment)?
HIPAA Notes:

a. Denial of Access: In accordance with 45 CFR Part 164 Subpart C § 164.524, covered entities may deny an individual access to their PHI under two conditions: unreviewable denials (see § 164.524(a)(2)) and reviewable denials (see § 164.524(a)(3)).

b. Denial of Amendments: In accordance with 45 CFR § 164.526(a), covered entities may deny requests to correct (or amend) PHI, if it determines that the PHI or record:

- **Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;**
- **Is not part of the designated record set;**
- **Would not be available for inspection under § 164.524; or**
- **Is accurate and complete.**

SAMPLE LANGUAGE: For PHI, in accordance with the HIPAA Privacy Rule, the **[name of entity] may deny an individual access** to his or her PHI for the following "unreviewable" and "reviewable" conditions:

- Unreviewable denial: Situations involving (i) psychotherapy notes, information compiled for use in legal proceedings, and certain information held by clinical laboratories; (ii) certain requests which are made by inmates of correctional institutions when providing such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates, or the safety of any officer, employee, or other person at the institution responsible for the transporting of the information; (iii) information created or obtained during research that includes treatment if certain conditions are met; (iv) denials permitted by the Privacy Act; and (v) information obtained from non-health-care providers pursuant to promises of confidentiality. See 45 CFR § 164.524(a)(2).

- Reviewable denial: Situations involving (i) disclosures which would cause endangerment of the individual or another person; (ii) when the PHI refers to another individual and disclosure is likely to cause substantial harm; and (iii) requests made by a personal representative where disclosure is likely to cause substantial harm. See 45 CFR § 164.524(a)(3).

Further, in accordance with HIPAA's Right to Amend, 45 CFR § 164.526(a), the entity **may deny requests to amend** PHI if it determines that the PHI or record:

- Was not created by the entity, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment.
- Is not part of the designated record set.
- Would not be available for inspection under § 164.524.
- Is accurate and complete.

If the **[name of entity]** denies the request, in whole or in part, the entity will provide the individual with a written denial.

A request for correction may be denied when the record is not retained by the entity; it is determined that the information in the record is accurate and complete; or the request for correction cannot be substantiated as to its accuracy or veracity (in such case, it is within the discretion of the agency to determine whether the proposed correction should be included in the record).

2. If requests for access or corrections (amendments) are denied, what is the entity's procedure for appeal (or review)?

HIPAA Notes:

a. Denial of Access Review: In accordance with 45 CFR § 164.524(a)(3) and (4), a covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed in the following circumstances: a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; the PHI makes reference to another person and the access is reasonably likely to cause substantial harm to such other person; or the request is made by the individual personal representative and is reasonably likely to cause substantial harm to the individual or another person.

b. In accordance with 45 CFR § 164.524(a)(4), if access is denied, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official.

c. Denial of Amendment Statement of Disagreement: In accordance with 45 CFR § 164.526(d), when a request to amend PHI is denied but the individual continues to dispute the accuracy of the information, covered entities must provide the individual with an opportunity to either file a statement of disagreement with the entity or to request that the entity provide the individual's request for amendment and the denial with any future disclosures of the PHI. In addition, the entity must provide documentation of that dispute with any subsequent disclosure of the disputed PHI.

The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the entity must provide a copy to the individual who submitted the statement of disagreement.

SAMPLE LANGUAGE: The individual who has requested access or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the **[name of entity]** or, if applicable, the originating agency. The individual will also be informed of the procedure for appeal (or review) when the entity or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

For denial of access to PHI, the individual will be informed of the procedure for requesting a review of the denial. The entity, upon receipt of a request to review the denial for access, will promptly refer the request to a designated licensed health-care professional, who was not directly involved in the original denial, to review the decision. The designated reviewing official will determine, within a reasonable period of time, whether or not to deny the request for access and the entity will promptly notify the individual of the decision in writing.

For denial of amendment (or changes) to the PHI, the individual will be informed of the procedure for filing a statement of disagreement and the option, instead of filing a statement of disagreement, to have the individual's request for amendment and the denial supplied with any future disclosures of the PHI. The entity, upon receipt of a statement of disagreement for a denied amendment, may prepare a written rebuttal

to the individual's statement of disagreement and, if such rebuttal is prepared, will provide a copy to the individual. In addition, the entity will link the individual's statement of disagreement, and, if any, the entity's rebuttal to the designated record set or may attach an accurate summary of any such information to any subsequent disclosure of the PHI to which the disagreement relates.

The entity will maintain a record of all requests for access or amendment and any requests for review or statements of disagreement and will include documentation of the request or dispute with any subsequent disclosure of the PHI.

L. Information Security Safeguards

HIPAA and 42 CFR Part 2 Security Requirements:

a. **HIPAA—In addition to the HIPAA Privacy Rule, the U.S. Department of Health and Human Services (HHS) developed the HIPAA Security Rule, or *Security Standards for the Protection of Electronic Protected Health Information*, a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and nontechnical safeguards that covered entities must put in place to secure individuals' "electronic protected health information" (e-PHI). The HIPAA Security Rule does not apply to PHI transmitted orally or in writing.[25]**

b. **The following security provisions, while they address the security safeguards and policies of all of the types of information the entity collects, receives, stores, accesses, shares, and disseminates, they also include provisions designed to meet the HIPAA Security Rule requirements, to assist those entities that are HIPAA-covered entities.**

c. **In accordance with 42 CFR Part 2 Subpart B § 2.16(b), programs shall adopt, in writing, procedures which regulate and control access to and use of written records which are subject to these regulations.**

   1. **Does your entity have a designated information security officer? Is training provided for the information security officer?**

      If the role is a component of another position, identify the title of the position upholding security officer responsibilities [for smaller agencies, this may be a role shared by partner agencies or regional entities].

      HIPAA Note: In accordance with 45 CFR Part 164 Subpart C § 164.308(a)(2), "HIPAA-covered entities" are required to designate a security official who is responsible for the development and implementation of security policies and procedures that are in compliance with 45 CFR Part 164 Security and Privacy.

      SAMPLE LANGUAGE: The **[name of entity]**'s **[insert position title]** is designated and trained to serve as the entity's information security officer.

   2. **What are your entity's physical, procedural, and technical safeguards for ensuring the security of entity data?**

      Describe how the entity will protect the information from unauthorized access, modification, theft, sabotage, or destruction (whether internal or external) resulting from natural or human-caused disasters or intrusions with, for example, procedures, practices, system protocols, use of software, information technology tools, processes for data backups, and physical security measures.

      Best Practice: Reference generally accepted industry or other applicable standard(s) for security with which the entity complies.

      HIPAA/42 CFR Part 2 Notes:

[25] Summary of the HIPAA Security Rule, www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.

a. **In accordance with 45 CFR Part 164 Subpart C § 164.308(a)(7)(ii), HIPAA-covered entities must:**

- **Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI (e-PHI);**
- **Develop a Disaster Recovery Plan to restore any loss of data, and**
- **Develop an Emergency Mode Operation Plan to enable continuation of critical business processes for protection of the security of e-PHI while operating in emergency mode.**

b. **In accordance with 45 CFR Part 164 Subpart C § 164.310 Physical safeguards, (a), a HIPAA-covered entity must implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. Further, covered entities must establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.**

c. **In accordance with 45 CFR Part 164 Subpart C § 164.312(a)(2)(ii), covered entities are required to establish procedures for obtaining necessary e-PHI during an emergency.**

d. **In accordance with 42 CFR Part 2 Subpart B § 2.16, written records which are subject to these regulations [42 CFR Part 2] must be maintained in a secure room, locked file cabinet, safe or other similar container when not in use and each program shall adopt in writing procedures which regulate and control access to and use of written records which are subject to these regulations.**

SAMPLE LANGUAGE: The **[name of entity]** will operate in a secure facility protected from external intrusion. The entity will utilize secure internal and external safeguards against network intrusions, including electronic measures to confirm that information, including e-PHI, has not been improperly altered or destroyed. Written records will be maintained in a secure room in a locked container (file cabinet, safe) and the entity, per established procedures, will regulate and control access to and use of the records. Access to the entity's databases from outside the facility will be allowed only over secure networks. For recovery purposes, the entity will ensure that data is backed up in a separate and secure environment and will establish and follow a Disaster Recovery Plan to restore any lost data, as well as an Emergency Mode Operation Plan to enable continuation of critical business processes, such as procedures for facility access, access to necessary e-PHI, and the protection of the security of e-PHI while operating in emergency mode.

3. **What requirements exist to ensure that the information will be stored in a secure format and a secure environment?**

SAMPLE LANGUAGE: The **[name of entity]** will store information in a manner that ensures that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

4. **If a HIPAA-covered entity, does the entity conduct an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the entity?**

HIPAA Note: In accordance with 45 CFR Part 164 Subpart C § 164.308, Administrative safeguards, a covered entity is required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity and must implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

SAMPLE LANGUAGE: The **[name of entity]** conducts assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the entity and implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

5. **What are the required credentials of entity personnel authorized to have access to entity information?**

HIPAA/42 CFR Part 2 Notes:

a. **In accordance with 45 CFR Part 164 Subpart E § 164.514(d)(2)(i), a HIPAA-covered entity must identify those persons or classes of persons, as appropriate, in its workforce who need access to**

PHI to carry out their duties and for each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

b. In accordance with 42 CFR Part 2 Subpart B § 2.12(c)(3), communication of information within the program (or to an entity with direct administrative control over the program) be limited to those persons who have a need for the information in connection with their duties that arise out of the provision of diagnosis, treatment or referral for treatment of substance abuse.

SAMPLE LANGUAGE: Access to **[name of entity]** information will be granted only to entity personnel whose positions and job duties require such access; who have successfully completed a background check, if applicable; and who have been selected, approved, and trained accordingly. All staff members are required to strictly adhere to the identification and access procedures established by the facility.

6. Does electronic access to entity data identify the user?
HIPAA Note: In accordance with 45 CFR Part 164 Subpart C § 164.312 technical safeguards, (a)(2)(i), HIPAA-covered entities are required to assign a unique name and/or number for identifying and tracking user identity.

SAMPLE LANGUAGE: Authorized queries made to the **[name of entity]**'s data applications will be logged into the data system identifying the user initiating the query, including the unique name and/or number assigned to each authorized individual.

7. Is a log kept of accessed and disseminated entity data, and is an audit trail maintained?

SAMPLE LANGUAGE: The **[name of entity]** will utilize electronic and/or paper logs to maintain audit trails of accessed, requested**,** or disseminated information, and of denied access due to nonauthorization.

8. Does the entity have electronic procedures for terminating an electronic session after a period of inactivity?

HIPAA Note: In accordance with 45 CFR Part 164 Subpart C § 164.312 Technical safeguards, (a)(2)(iii), a HIPAA-covered entity must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

SAMPLE LANGUAGE: To prevent access by unauthorized individuals, the **[name of entity]** will institute electronic procedures whereby electronic sessions will terminate after a predetermined period of inactivity.

9. Are risk and vulnerability assessments (if maintained) stored separately from publicly available data?

SAMPLE LANGUAGE: To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

10. What are the entity's procedures for responding to suspected or known security incidents?

HIPAA Note: In accordance with 45 CFR Part 164 Subpart C § 164.308(a)(6)(ii), HIPAA-covered entities must identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

SAMPLE LANGUAGE: The **[name of entity]** will identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity; and document security incidents and their outcomes.

11. What are the entity's procedures for adhering to data breach notification laws or policies?

Best Practice: Provide notification to originating agencies when PHI they provided to the entity has been the subject of a suspected or confirmed data breach.

HIPAA Notes:

a. Section 1178 of the Social Security Act, 42 U.S.C. 1320d-7 provides that HIPAA administrative simplification provisions generally preempt conflicting State law. As such, State law covering

breaches of PHI that is contrary to HIPAA is preempted by HIPAA breach notification regulations. (See "Contrary" in Appendix B. Terms and Definitions.)

b. In accordance with 45 CFR Part 164 Subpart D–Notification in the Case of Breach of Unsecured Protected Health Information § 164.404(a)(1), a covered entity shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been accessed, acquired, used, or disclosed as a result of such breach.

c. In accordance with 45 CFR Part 164 Subpart D § 164.404(b), except as provided in § 164.412 regarding a law enforcement delay where a notification would impede an ongoing criminal investigation or cause damage to national security, a covered entity shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

d. In accordance with 45 CFR Part 164 Subpart C § 164.530(f), a covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures by the covered entity or its business associate.

SAMPLE LANGUAGE, Option 1:

[For use if there is no applicable state data breach notification law and you choose not to follow the Office of Management and Budget (OMB) guidance in Option 2.] The **[name of entity]** will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

SAMPLE LANGUAGE, Option 2:

[For use if there is no applicable state data breach notification law and you choose to follow the OMB guidance.] The **[name of entity]** will follow the data breach notification guidance set forth in OMB Memorandum M-07-16 (May 2007, see http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf).

SAMPLE LANGUAGE, Option 3:

[For use if there is an applicable state data breach notification law.] The **[name of entity]** will follow the data breach notification guidance set forth in **[cite applicable law]**.

Breach of Protected Health Information: For covered entities, add the following language regarding breach of PHI to any of options listed above:

For PHI, the **[name of entity]**, following the discovery of a breach of unsecured PHI, will and without unreasonable delay and in no case later than 60 calendar days after discovery of the breach:

- Notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been accessed, acquired, used, or disclosed as a result of such breach.

- Mitigate, to the extent practicable, any harmful effect that is known to the entity of a use or disclosure of PHI in violation of entity policies and procedures by the entity or its business associate(s),

- For breaches affecting fewer than 500 individuals within a state or particular jurisdiction, maintain a log of all such breaches occurring during the year and, no later than 60 days after the end of the calendar year in which the breaches were discovered, submit such log to the Secretary of HHS. Logs will be kept for a minimum of six years.

- For breaches affecting more than 500 individuals within a state or particular jurisdiction, notify the Secretary of HHS immediately and prominent media outlets serving the state or jurisdiction.

Further, business associates shall, following the discovery of a breach of unsecured PHI, notify [**name of entity**] of such breach without unreasonable delay and in no case later than 60 calendar days after discovery

of a breach. Per § 164.404, the [**name of entity**] ultimately maintains the obligation to notify affected individuals of the breach.

All notifications made by the [**name of entity**] or its business associates will be made in the manner specified by the U.S. Department of Health and Human Services (HHS) Web site: www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/.

Best-practice sample language applicable to all three options [add after the entity's breach notification language, whether Option 1, 2, or 3 is chosen]: **[To the extent allowed by the [insert state, if there is a state law] data breach notification law]** The **[name of entity]** will immediately notify the originating agency from which the entity received personal information of a suspected or confirmed breach of such information.

M. Information Retention and Destruction

1. What is your entity's review schedule for validating or purging information? Specify periodic basis and/or reference the applicable law.

HIPAA/42 CFR Part 2 Notes:

a. HIPAA regulations do not include medical record retention requirements. Instead, state law regarding record retention applies.

b. The average length of retention ranges between five to seven years.

c. The Centers for Medicare and Medicaid Services (CMS) requires that patient records for Medicare beneficiaries be retained for a period of 5 years (see 42 CFR 482.24 (b)). Medicaid requirements may vary by state. Entities should refer to state law for specific state requirements.

SAMPLE LANGUAGE: All applicable information, including e-PHI, will be reviewed for record retention (validation or purge) by **[name of entity]** at least every five years [**or insert alternate time period**] [**or for a longer or shorter period as specified by state law, local ordinance, or applicable policy**].

2. What is your entity's retention and destruction policy? Describe the methods employed to remove or destroy PHI.[26] Reference law or policy, if applicable.

Best Practice: A retention and destruction policy should be provided for all PHI databases/records held by the entity.

HIPAA Note: In accordance with 45 CFR Part 164 Subpart C § 164.310 Physical safeguards, (d)(2), HIPAA-covered entities are required to implement policies and procedures to address the final disposition of e-PHI, and/or the hardware or electronic media on which it is stored. In addition, covered entities must implement procedures for removal of e-PHI from electronic media before the media are made available for re-use.

SAMPLE LANGUAGE: When information has no further value, its retention period has expired, it meets the criteria for removal according to the **[name of entity]**'s retention and destruction policy or according to applicable law **[if such a law, cite the law or remove the phrase "applicable law"]**, or as agreed upon with the originating entity in a participation membership agreement, it will be purged, destroyed, and deleted. For paper records, the entity will shred, burn, pulp, or pulverize the records so that personally identifiable and protected health information is rendered unreadable, indecipherable, and otherwise cannot be reconstructed. In addition, the entity will remove e-PHI from any hardware or electronic media on which it was stored prior to making the media available for reuse.

3. Is a record kept of dates when information is to be removed (purged) if not validated prior to the end of its period? Is notification given prior to removal (for example, an autogenerated system prompt to entity personnel that a record is due for review and validation or purge)?

[26] *Frequently Asked Questions About the Disposal of Protected Health Information*, U.S. Department of Health and Human Services, Office for Civil Rights, www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf.

SAMPLE LANGUAGE: A record of information to be reviewed for retention will be maintained by the **[name of entity]**.

4. Is a confirmation of the deletion required?

SAMPLE LANGUAGE: A printed or electronic confirmation of the deletion will be kept by the entity that includes a log of the deletion (e.g., date of deletion).

N. Accountability and Enforcement

N.1 Information System Transparency

1. Is your entity's PHI privacy policy available to the public?

SAMPLE LANGUAGE: The **[name of entity]** will be open with the public in regard to PHI collection, maintenance, and sharing practices. The entity's PHI privacy policy will be provided to the public for review, made available upon request, and posted on the entity's Web site **[or Web page]** at **[insert Web address]**.

2. For HIPAA-covered entities, does your entity post its PHI privacy policy on the entity's Web site?

HIPAA Notes:

a. In accordance with 45 CFR Part 164 Subpart C § 164.520, individuals have a right to adequate notice by the covered entity, of the uses and disclosures of PHI that may be made by the entity and of the individual's rights and the covered entity's legal duties with respect to PHI. However, in accordance with § 164.520(a)(3), an inmate does not have a right to notice under this section and the requirements do not apply to a correctional institution that is a covered entity.

b. In accordance with 45 CFR § 164.520(c)(3), any entity that maintains a Web site that provides information about its services or benefits must prominently post its notice [for HIPAA, privacy practices for PHI] on the site and make it available electronically through the site.

SAMPLE LANGUAGE: The **[name of entity]** will post the entity's PHI privacy policy on the entity's Web site at **[insert Web address]**.

3. For federally assisted programs, does the entity provide a notice to patients of federal confidentiality requirements?

42 CFR Part 2 Note: In accordance with 42 CFR Part 2 Subpart B § 2.22, at the time of admission or as soon thereafter as the patient is capable of rational communication, each program shall communicate to the patient that federal law and regulations protect the confidentiality of substance abuse patient records and give to the patient a summary in writing of the federal law and regulations that is in compliance with the written summary requirements outlined in § 2.22(b). (See Appendix G. 42 CFR 2.22: Notice To Patients of Federal Confidentiality Requirements.)

SAMPLE LANGUAGE: The **[name of entity]** will, for individuals tested, diagnosed, and/or treated for substance abuse, provide the individual with a notice of federal confidentiality requirements of substance abuse patient records.

4. Does your entity have a process for individuals to make complaints concerning the entity's policies, procedures, and privacy practices if the individual feels that a violation of HIPAA or 42 CFR Part 2 has occurred?

HIPAA/42 CFR Part 2 Notes:

a. In accordance with 45 CFR § 164.530(d), a covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures and must document all complaints received and their disposition, if any.

b. In accordance with 45 CFR Part 160 Subpart C § 160.306, a person who believes the entity is not complying with HIPAA may file a complaint with the Secretary of the U.S. Department of Health

and Human Services (www.hhs.gov/ocr/privacy/hipaa/complaints/index.html). Complaints must meet the following requirements:

- **A complaint must be filed in writing, either on paper or electronically.**
- **A complaint must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s).**
- **A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.**
- **The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.**

c. In accordance with 42 CFR Part 2 Subpart A § 2.5, the report of any violation of 42 CFR Part 2 regulations may be directed to the United States Attorney for the judicial district in which the violation occurs. The report of any violation by a methadone program may be directed to the Regional Offices of the Food and Drug Administration.

SAMPLE LANGUAGE: Individuals who have complaints regarding the **[name of entity]**'s general policies and procedures may contact the **[name of entity]**'s [**privacy officer or other position title or office**] at [**insert contact information**]. The entity will maintain a record of all complaints received regarding the entity's policies and procedures and any action taken, thereof.

Individuals who believe the **[name of entity]** is not complying with HIPAA may file a complaint with the Secretary of the U.S. Department of Health and Human Services (www.hhs.gov/ocr/privacy/hipaa/complaints/index.html). Complaints must meet the following requirements:

- A complaint must be filed in writing, either on paper or electronically.
- A complaint must name the person who is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s).
- A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.
- The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

Individuals may report any violations of 42 CFR Part 2 regulations regarding the handling of substance abuse information to the United States Attorney for the judicial district in which the violation occurs. The report of any violation by a methadone program may be directed to the Regional Offices of the Food and Drug Administration.

5. Does your entity have a point of contact for handling inquiries or complaints?

SAMPLE LANGUAGE: The **[name of entity]**'s **[privacy officer or other position title]** will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the entity. The **[privacy officer or other position title]** can be contacted at **[insert mailing address or e-mail address]**.

N.2 Accountability

1. Does access (e.g., electronic or hard-copy access) to the entity's data identify the user? Is the identity of the user retained in an audit log?

SAMPLE LANGUAGE: The audit log (whether electronic or paper) of access (or queries) to the [name of entity's] information will identify the user.

2. **Is a log (whether electronic or paper) kept of accessed and disseminated entity-held data, and is an audit trail maintained?**

   SAMPLE LANGUAGE: The **[name of entity]** will maintain an audit trail of accessed, requested**,** or disseminated information and of denied access due to nonauthorization. An audit trail will be kept for a minimum of **[specify the retention period for your jurisdiction/entity for this type of request]** of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

3. **What procedures and practices does your entity follow to enable evaluation of user compliance with information access requirements, the entity's PHI privacy policy, and applicable law?**

   SAMPLE LANGUAGE: The **[name of entity]** will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with information access requirements and with the provisions of this PHI privacy policy and applicable law. This will include logging access to this information and periodic auditing, so as not to establish a pattern of the audits. These audits will be mandated at least **[quarterly, semiannually, or annually]**, and a record of the audits will be maintained by the **[privacy officer or title of designee]** of the entity.

4. **Does your entity have a mechanism for entity personnel to report errors and suspected or confirmed violations of entity privacy policies related to PHI?**

   SAMPLE LANGUAGE: The **[name of entity]**'s personnel or other authorized users shall report errors and suspected or confirmed violations of entity privacy policies relating to PHI to the entity's privacy officer. **[Cross-reference to policy (see Section C.3).]**

5. **What is the entity's retention period for patient consent authorizations, and are audits completed to ensure that appropriate consent authorizations are maintained and current?**

   SAMPLE LANGUAGE: Per 45 CFR § 164.508(b)(6), the **[name of entity]** will keep a copy of each signed consent-to-release authorization form for six years from its expiration date. The **[name of entity]** will periodically audit and inspect "consent-to-release" authorizations to ensure that an individual's PHI, 42 CFR Part 2, and other protected information the individual has consented to release to the entity are maintained and current.

6. **Are audits of user compliance completed by an independent third party or a designated representative of the entity? Are the audits conducted both annually and randomly?**

   <u>42 CFR Part 2 Notes</u>:

   a. **In accordance with 42 CFR Part 2 Subpart D § 2.53(a) for substance abuse information, if patient records are not copied or removed, patient identifying information may be disclosed in the course of a review of records on program premises to any person who agrees in writing to comply with the limitations on redisclosure and who performs the audit or evaluation activity (on behalf of any federal, state, or local governmental agency which provides financial assistance to the program or is authorized by law to regulate its activities or any private person which provides financial assistance to the program, which is a third-party payer covering patients in the program, or which is a quality improvement organization performing a utilization or quality control review) or is determined by the program director to be qualified to conduct the audit or evaluation activities.**

   b. **In accordance with 42 CFR Part 2 Subpart D § 2.53(b), records containing patient identifying information may be copied or removed from program premises by any person who agrees in writing to maintain the patient identifying information in accordance with the security requirements provided in § 2.16 (or more stringent requirements); destroy all the patient identifying information upon completion of the audit or evaluation; and comply with the limitations on disclosure and use of this regulation; and performs the audit or evaluation activity on behalf of the entities described in a. above.**

   c. **In accordance with 42 CFR Part 2 Subpart D § 2.53(d), except as provided in Medicare or Medicaid audits, patient identifying information disclosed [for purposes of audit or evaluation] may be disclosed only back to the program from which it was obtained and used only to carry**

out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by a court ordered entered under § 2.66.

Entities that are subject to both HIPAA and 42 CFR Part 2 must combine the regulations requirements. Three options result:

- **If the audit or evaluation is conducted by the entity/program or its employees (an internal audit), it is permissible under both sets of regulations; no patient consent or authorization is required, per 45 CFR § 164.502(a)(1)(ii) and 42 CFR Part 2 Subpart B § 2.12(c)(3).**

- **If the audit or evaluation is conducted by a "health oversight agency," the entity/program may disclose patient identifying information so long as the health oversight agency makes the written commitments required by 42 CFR Part 2 Subpart D § 2.53(d) and the disclosure meets the requirements in 45 CFR § 164.512(d). If the health oversight agency copies or removes patient records from the entity/program, it must agree in writing to abide by the requirements of 42 CFR Part 2 Subpart D § 2.53(b).**

- **If an audit or evaluation is conducted by an outside entity on behalf of the program as opposed to a health oversight agency, the program must have a signed business associate agreement (BAA) with the auditor or evaluator that satisfies the requirements of both HIPAA and 42 CFR Part 2 by incorporating either the necessary 42 CFR Part 2 Qualified Service Organizations Agreement (QSOA) requirements or the appropriate provisions of 42 CFR Part 2 Subpart D § 2.53.**

SAMPLE LANGUAGE: The **[name of entity]** will annually conduct an audit and inspection of the information contained in its information system(s) to enable evaluation of user compliance. The audit will be conducted by the entity's **[designated audit committee, office, or position] (or) [a designated independent panel]** and will, for substance abuse information, comply with 42 CFR Part 2 Subpart D § 2.53 audit and evaluation requirements. This **[committee/office/position] (or) [independent panel]** has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the entity. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the entity's information.

7. **How often do you review and update the provisions contained within this PHI privacy policy (for example, annually)? Is a record kept of all changes to entity PHI privacy policies, including security provisions and procedures and, if so, what is the entity's retention period for such documentation?**

   HIPAA Notes:

   a. **In accordance with 45 CFR Part 164 Subpart C § 164.316(a) and (b), a HIPAA-covered entity may change its policies and procedures at any time, provided that the changes are documented and implemented. Covered entities must maintain the policies and procedures in written (which may be electronic) form, and will maintain a written (which may be electronic) record of revisions or policy changes (e.g., action, activity, or assessment). Covered entities are required to retain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. The documentation must be made available to those persons responsible for implementing the procedures to which the documentation pertains. Finally, covered entities are required to review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the e-PHI.**

   b. **In accordance with 45 CFR Part 164 Subpart C § 164.530(i)(2)(i), a covered entity must change its policies and procedures as necessary and appropriate to comply with changes in law, including HIPAA standards, requirements, and implementation specifications.**

   c. **In accordance with 45 CFR Part 164 Subpart C § 164.530(i)(3), whenever there is a change in law that necessitates a change to the covered entity's policies and procedures, the entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the [privacy practices] notice required by § 164.520, the entity must promptly make the appropriate revisions to the privacy notice in accordance with § 164.520(b)(3).**

SAMPLE LANGUAGE: The **[name of entity]**'s privacy committee or privacy officer will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this PHI privacy policy at least annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations. The entity will document and retain a record of each policy and procedural change for six years from the date of its creation or the date when it last was in effect, whichever is later.

N.3 Enforcement

1. **What are your procedures for enforcement if entity personnel, a participating agency, or an authorized user is suspected of being or has been found to be in noncompliance with the provisions of this policy?**

   HIPAA/42 CFR Part 2 Notes:

   a. **In accordance with 45 CFR Part 164 Subpart C § 164.308(a)(1)(ii)(C), HIPAA-covered entities must apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. In addition, § 164.530(e)(1) and (2), HIPAA-covered entities must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity and must document the sanctions that are applied, if any.**

   b. **In accordance with 42 CFR Part 2 Subpart A § 2.4, Criminal penalty for violation, any person who violates any provision of these regulations shall be fined not more than $500 in the case of a first offense, and not more than $5,000 in the case of each subsequent offense.**

   SAMPLE LANGUAGE: If entity personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this PHI privacy policy regarding the gathering, collection, use, retention, security, destruction, sharing, classification, or disclosure of PHI, the **[title of entity director]** of the **[name of entity]** will:

   - Suspend or discontinue access to information by the entity personnel, the participating agency, or the authorized user.
   - Suspend, demote, transfer, or terminate entity personnel, as permitted by applicable personnel policies.
   - Apply administrative actions or sanctions as provided by [state entity or agency] rules and regulations or as provided in entity/agency personnel policies.
   - If the authorized user is from an agency external to the entity, request that the user's employer initiate disciplinary proceedings to enforce the policy's provisions.
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

   The **[name of entity]** will document any sanctions that are applied.

2. **What is the entity's policy with regard to the qualifications and number of participating agency personnel authorized to access PHI, and what additional sanctions are available for violations of the entity's PHI privacy policy?**

   SAMPLE LANGUAGE: The **[name of entity]** reserves the right to restrict the qualifications and number of personnel having access to PHI and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the entity's privacy policy.

O. Training

1. **What personnel does your entity require to participate in training programs regarding implementation of and adherence to this privacy policy?**

   HIPAA Notes: HIPAA requires that all workforce members be trained regarding the entities privacy and security policies.

a. **In accordance with 45 CFR § 164.530(b)(1), a covered entity must train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.**

b. **In accordance with 45 CFR § 164.530(b)(2)(ii), a covered entity must document that the training has been provided.**

SAMPLE LANGUAGE: The **[name of entity]** will require the following individuals to participate in training programs regarding implementation of and adherence to the entity's PHI privacy policy, including security provisions:

- All assigned personnel of the entity.
- Personnel providing information technology services to the entity.
- Staff in other public agencies or private contractors providing services to the entity.
- Authorized users who are not employed by the entity or a contractor.

The entity maintains a record of all training that is provided.

2. **What is covered by your training program (for example, purpose of the policy, substance and intent of the provisions of the policy, security requirements, impact of infractions, and possible penalties for violations)?**

SAMPLE LANGUAGE: The **[name of entity]**'s privacy policy training program will cover:

- Purposes of the privacy, civil rights, and civil liberties protection policy.
- Security awareness training for covered entities, per 45 CFR § 164.308(a)(5)(i).
- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the [**name of entity**], as well as breach notification requirements and procedures.
- Originating and participating agency responsibilities and obligations under applicable law and policy.
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user.
- The potential impact of violations of the entity's privacy policy.
- Mechanisms for reporting violations of entity privacy protection policies and procedures.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

Appendix A—Glossary of Terms and Definitions

The following is a list of primary terms and definitions used throughout this template. These terms are also useful in drafting the definitions section of the entity's privacy policy.

Access—having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Agency—A participating agency that accesses, contributes, and/or shares information in the **[name of entity]**'s information system.

Alcohol Abuse—Per 42 CFR Part 2 Subpart A § 2.11, alcohol abuse means the use of an alcoholic beverage which impairs the physical, mental, emotional, or social well-being of the user. For the purposes of this document, the term "substance abuse" will include both alcohol abuse and drug abuse.

Amending Data—Per § 164.526 (A)(1), An individual has the right to have a covered entity amend [or correct] PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set. See Corrections (PHI Data).

Anonymized—Previously identifiable data that has been deidentified and for which a code or other link no longer exists. An investigator would not be able to link anonymized information back to a specific individual.

Anonymous—Data that was collected without identifiers and that was never linked to an individual. Identifiable coded data is not anonymous but rather may be maintained confidentially.

Audit Trail—A generic term for recording (logging) a sequence of activities, whether electronic or paper. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc. In a paper-based logging system, this includes recording a sequence of activities such as who requested the information and what was information was provided to them.

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—The process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina

or iris), finger (fingertip, thumb, finger length, or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Breach—Per 45 CFR Part 164—Security and Privacy, Subpart D, § 164.402 Definitions, "breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI.

1. (i) For purposes of this definition, *compromises the security or privacy of the PHI* means poses a significant risk of financial, reputational, or other harm to the individual.

   (ii) A use or disclosure of PHI that does not include the identifiers listed at § 164.514(e)(2), date of birth, and ZIP code does not compromise the security or privacy of the PHI.

2. Breach excludes:

   (i.) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

   (ii.) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health-care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

   (iii.) A disclosure of PHI where a covered entity or business associate has a good-faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

See Unsecured Protected Health Information.

Business Associate—Per 45 CFR Part 160 General Administrative Requirements, Subpart A, § 160.103 Definitions, means, with respect to a covered entity, that a business associate is:

1. A person or entity who, on behalf of such covered entity or of an organized health-care arrangement (as defined in § 164.501) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

   - A function or activity involving the use or disclosure of PHI , including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

   - Patient safety activities, in accordance with the Patient Safety and Quality Improvement Act of 2005 (PSQIA), 42 U.S.C. 299b-21, et seq.; or

   - A function or activity involving the creation, receipt, maintenance, or transmission of PHI on behalf of a covered entity; or

   - Any other function or activity regulated by this subchapter; or

2. A person or entity who provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health-care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of PHI from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

   A covered entity participating in an organized health-care arrangement that performs a function or activity as described in 1. of this definition for or on behalf of such organized health-care arrangement, or that provides a service as described in 2. of this definition to or for such organized health-care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health-care arrangement.

3. A Patient Safety Organization (PSO) who receives reports of patient safety events or concerns from providers and provides analyses of events to reporting providers. A reporting provider may be a HIPAA-covered entity and, thus, information reported to a PSO may include PHI that the PSO may analyze on behalf of the covered provider. The analysis of such information is a patient safety activity for purposes of PSQIA and the Patient Safety Rule, 42 CFR 3.10, et seq. HIPAA rules treat a PSO as a business associate when the PSO is performing the quality analyses and other activities on behalf of a covered health-care provider.

4. In accordance with the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Section 13408, a Health Information Organization, E-prescribing Gateway, or other

person that provides data transmission services with respect to PHI to a covered entity and that requires routine access to such PHI; and a person who offers a personal health record to one or more individuals on behalf of a covered entity.

5. A personal health record vendor that maintains PHI on behalf of the covered entity (for the benefit of the individual) and has access to PHI, regardless of whether the personal health record vendor actually exercises this access.

6. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate. See Subcontractor.

7. A person or entity that meets the definition of a business associate even if the covered entity (or business associate with respect to a subcontractor) fails to enter into the required business associate contract with the person or entity.

8. A covered entity may be a business associate of another covered entity. See Covered Entity.

Entities that act as mere conduits for the transport of PHI (e.g., U.S. Postal Service or United Parcel Service and their electronic equivalents, such as Internet service providers providing mere data transmission services), but do not access the information other than on a random or infrequent basis, as necessary to perform the transportation service or as required by law, **are not business associates**. For example, a telecommunications company may have occasional, random access to PHI when it reviews whether the data transmitted over its network is arriving at its intended destination. Such occasional, random access to PHI would not qualify the company as a business associate.

When a covered entity disclosed PHI to a health-care provider concerning the treatment of an individual, in which a covered entity **is not required to enter into a business associate contract** or other arrangement with the recipient of the PHI, the recipient in these circumstances **is not considered a business associate**.

In accordance with the HITECH Act, Subtitle D-Privacy, PART 1—Improved Privacy Provisions and Security Provisions, Section 13401, the security administrative, physical, and technical safeguards requirements in 45 CFR Part 164 Subpart C §§ 164.306, 164.308, 164.310, and 164.312, as well as the HIPAA Security Rule's policies and procedures and documentation requirements in § 164.316, apply to business associates in the same manner as these requirements apply to covered entities, and that business associates are civilly and criminally liable for violations of these provisions.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "civil liberties" refers to fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments—to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights—The term "civil rights" refers to those rights and privileges of citizenship and equal protection that the state is constitutionally bound to guarantee all citizens regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Protection of civil rights imposes an affirmative obligation upon government to promote equal protection under the law. These civil rights to personal liberty are guaranteed to all U.S. citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.

Community Health or Behavioral Health Provider—means a person, government agency, or body of persons (whether corporate or unincorporated) who or which:

- Provides a service in the community, such as medical, behavioral, or substance abuse treatment; or
- Holds himself, herself or itself out as being able to provide a service in the community.

In the corrections field, community health or behavioral health providers provide treatment services or programs to individuals released from prison, or jail or under community supervision (i.e., pre-trial, probation, parole, community corrections).

Computer Security—The protection of information assets through the use of technology, processes, and training.

Confidentiality—Closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Continuity of Care—Means the experience of both recipients and providers that everyone involved in the care process is working together across settings and throughout the course of illness to address the unique needs and preferences of an individual patient and family.

Contrary—When used to compare a provision of state law to a HIPAA standard, requirement, or implementation specification, means:

1. A covered entity or business associate would find it impossible to comply with both the state and federal requirements; or

2. The provision of state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

Corrections (PHI Data)—When an entity identifies PHI that is erroneous, misleading, obsolete, or otherwise unreliable, the entity will either correct, flag, or amend the PHI. See Amending Data.

Correctional Institution—Per 45 CFR Part 164 Subpart C § 164.501 Definitions, is defined as any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered Entity—Per 45 CFR Part 160 General Administrative Requirements, Subpart A, § 160.103 Definitions, is defined as:

- A health plan;

- A health-care clearinghouse;

- A health-care provider who transmits any health information in electronic form in connection with a covered transaction [relating to health claim report, status, payment, etc.].

Mental health treatment providers, either in the community or as a unit in a jail, will ordinarily be covered entities. An organization that is a covered entity is subject to HIPAA's minimum level of restrictions for sharing PHI. A covered entity is subject to HIPAA for all communications, regardless of whether the information is transmitted electronically in a given case.[27]

Credentials—Information that includes identification and proof of identification that are used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile entity or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Deidentified—Under the HIPAA Privacy Rule, data is de-identified if either (1) an experienced expert determines that the risk that certain information could be used to identify an individual is "very small" and documents and justifies the determination or (2) the data does not include any of the following 18 identifiers (of the individual or his or her relatives, household members, or employers) which could be used alone or in combination with other information to identify the subject: names; geographic subdivisions smaller than a state (including ZIP code); all elements of dates except year (unless the subject is greater than 89 years old); telephone numbers; fax numbers; e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers, including license plates; device identifiers and serial numbers; URLs; Internet protocol addresses; biometric identifiers; full-face photos and comparable images; and any unique identifying number, characteristic, or code. Note that even if these identifiers are removed, the Privacy Rule states that information will be considered identifiable if the covered entity knows that the identity of the person may still be determined.

Designated Record Set—Per 45 CFR Part 164 Subpart C § 164.501 Definitions, is defined as a group of records maintained by or for a HIPAA-covered entity that are:

- The medical records and billing records about individuals maintained by or for a covered health-care provider;

- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

[27] *Information Sharing in Criminal Justice—Mental Health Collaborations: Working with HIPAA and Other Privacy Laws*, John Petrila, J.D., L.L.M, and Fader-Towe, J.D., Council of State Governments Justice Center, Bureau of Justice Assistance, Office of Justice Programs, DOJ, www.bja.gov/Publications/CSG_CJMH_Info_Sharing.pdf

- Used, in whole or in part, by or for the covered entity to make decisions about individuals.

For purposes of this paragraph, the term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a HIPAA-covered entity.

Directly Identifiable—Any information that includes personal identifiers.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, entity, or organization outside the entity that collected it. Disclosure is an aspect of privacy focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Per 42 CFR Part 2 Subpart A § 2.11, "disclose" or "disclosure" means a communication of patient identifying information, the affirmative verification of another person's communication of patient identifying information, or the communication of any information from the record of a patient who has been identified.

Drug Abuse—Per 42 CFR Part 2 Subpart A § 2.11, drug abuse means the use of a psychoactive substance for other than medicinal purposes that impairs the physical, mental, emotional, or social well-being of the user. For the purposes of this document, the term "substance abuse" will include both alcohol abuse and drug abuse.

Electronic Media—Per 45 CFR Part 160 General Administrative Requirements, Subpart A, § 160.103 Definitions, means:

- Electronic storage material including, for example, memory devices in computers (hard drives) and any removable or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
- Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before transmission.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Electronic Medical Record—A computer-based record containing health-care information. This record may contain some, but not necessarily all, of the information that is in an individual's paper-based medical record. One goal of HIPAA is to protect identifiable health information as the system moves from a paper-based to an electronic medical record system.

Electronic Protected Health Information (e-PHI)—See paragraph 1. of the definition of Protected Health Information.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Entity—The **[name of entity],** which is the subject and owner of the privacy policy.

Fair Information Principles—The Fair Information Principles (FIPs) are contained within the Organisation for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated information systems. Some of the individual principles may not apply in all instances of an integrated information system.

The eight FIPs are:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

Family Member—Per 42 U.S.C. 300gg-91, as amended by GINA section 102(a)(4), means, with respect to any individual:

1. A dependent of such individual;

2. Any other individual who is a first-degree, second-degree, third-degree, or fourth-degree relative of such individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are to be treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor) and that, in determining the degree of relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

Federally Assisted—Defined in 42 CFR Part 2 as deriving some benefit from the U.S. government, such as accepting Medicaid payments or receiving nonprofit status under the federal tax code.

Under the regulations, programs also are federally assisted if they are conducted by a U.S. department or agency, are being carried out under authorization granted by a U.S. department or agency (such as Medicare providers, authorized methadone maintenance treatments, registration to dispense a substance under the Controlled Substances Act), or are supported by funds provided by any department or agency of the United States (including financial assistance that does not directly pay for the substance abuse diagnosis, treatment, or referral activities, or state or local government units that receive federal funds that could be used for substance abuse treatment). A program is also federally assisted if income tax deductions are granted to those who contribute to the program or if the program itself is tax-exempt. Under this definition, a private practitioner providing substance abuse treatment will not be a "program" within 42 CFR Part 2 unless the practitioner meets one of the conditions above; for example, through accepting Medicaid reimbursement.[28] See Program for more information.

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

General Information or Data—Information that may include records, documents, or files pertaining to protected health information, correctional entity operations information, incident data, and offender management and reentry information, and other general types of corrections (including pre-trial, probation, and parole) information. This may be information that is maintained in a records management system for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Genetic Information—Per the Genetic Information Nondiscrimination Act of 2008, Public Law 110-233, 122 Stat. 881, genetic information means, with respect to any individual, information about:

1. Such individual's genetic tests (see Genetic Tests);

2. The genetic tests of family members of such individual; and

3. The manifestation of a disease or disorder in family members of such individual (i.e., family medical history). (See Manifested or Manifestation.)

Genetic information includes, with respect to any individual, any request for or receipt of genetic services (see Genetic Services) or participation in clinical research that includes genetic services by such individual or family member of such individual.

Further, genetic information includes, with respect to an individual or family member of an individual who is a pregnant woman, the genetic information of any fetus carried by such pregnant woman and, with respect to an individual or family member utilizing an assisted reproductive technology, the genetic information of an embryo legally held by the individual or family member.

Genetic information does not include information about the sex or age of any individual.

Genetic Services—Genetic services means:

1. A genetic test;

2. Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

3. Genetic education.

Genetic Test—Per § 160.103, a genetic test is defined as an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes.

A genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Health Care—Per 45 CFR Part 160 General Administrative Requirements, Subpart A, § 160.103 Definitions, means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

[28] Ibid.

Health-Care Operations—Per 45 CFR Part 164 Subpart C § 164.501 Definitions, a health-care operation is defined as any of the following activities of the HIPAA-covered entity to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including outcome evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health-care costs, protocol development, case management and care coordination, contacting of health-care providers and patients with information about treatment alternatives; patient safety activities, in line with the Patient Safety and Quality Improvement Act of 2005 (PSQIA), 42 U.S.C. 299b-22(i) and 3.20; and related functions that do not include treatment;

2. Reviewing the competence or qualifications of health-care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health-care providers, training of non-health-care professionals, accreditation, certification, licensing, or credentialing activities;

3. Underwriting (Per GINA Title 1 and § 164.502(a)(3), health plans are prohibited from using or disclosing genetic information for underwriting purposes), premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable;

4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

6. Business management and general administrative activities of the entity, including, but not limited to:

    - Management activities relating to implementation of and compliance with the requirements of this subchapter;
    - Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer;
    - Resolution of internal grievances;
    - The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
    - Consistent with the applicable requirements of §164.514, creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health Care Provider—Per 45 CFR Part 164 Subpart C §164.501 Definitions, is defined as a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information—Per 45 CFR Part 164 Subpart C § 164.501 Definitions, is defined as any information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health-care provider, health plan, public health authority, employer, life insurer, school or university, or health-care clearinghouse; and

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Further, in accordance with § 160.103 and in compliance with the Genetic Information Nondiscrimination Act of 2008, Public Law 110-233, 122 Stat. 881, health information includes genetic information and is protected by the HIPAA privacy rule to the extent that such information is individually identifiable and held by a covered entity (subject to the general exclusions from the definition of PHI).

Health Oversight Agency—Per 45 CFR § 164.501, is an agency or authority of the United States, a state, a territory, a political subdivision of a state or a territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such a public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health-care system (whether public or private) or government programs in which health information is

necessary to determine eligibility or compliance or to enforce civil rights laws for which health information is relevant. Disclosures to health oversight agencies when an individual is the subject of the investigation are prohibited under certain circumstances by HIPAA's Privacy Rule, 45 CFR § 064.512(d)(2).

HIPAA—The Health Insurance Portability and Accountability Act of 1996. HIPAA is a federal law that was designed to allow portability of health insurance between jobs. In addition, it required the creation of a federal law to protect personally identifiable health information; if that did not occur by a specific date (which it did not), HIPAA directed the Department of Health and Human Services (DHHS) to issue federal regulations with the same purpose. DHHS has issued HIPAA privacy regulations (the HIPAA Privacy Rule) as well as other regulations [, such as the HIPAA Security Rule,] under HIPAA.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

Indirectly Identifiable—Data that do not include personal identifiers, but link the identifying information to the data through use of a code.

Individually Identifiable Health Information—See Protected Health Information.

Individual Responsibility—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists.

Information Quality (IQ)—Refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of IQ have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, IQ is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Inmate—Means a person incarcerated in or otherwise confined to a correctional institution. See Correctional Institution.

Invasion of Privacy—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Law—As used by this policy, law includes any local, state, or federal constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or entities.

Law Enforcement Official—Means an officer or employee of any agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or

2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Lawful Custody—See Correctional Institution.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—A necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Manifested or Manifestation—With respect to a disease, disorder, or pathological condition, manifested or manifestation means that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health-care professional with appropriate training and expertise in the field of medicine involved. A disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

Medical Emergency—Per 42 CFR § 2.51(a), a medical emergency is simply defined as a health emergency affecting any individual who requires immediate medical intervention.

Metadata—In its simplest form, metadata is information (data) about information—more specifically, information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counterterrorism activity, such as to further an investigation or meet another law enforcement requirement.

Nonrepudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

Originating Entity—The entity or organizational entity that documents information or data.

Parole—The release of a prisoner from incarceration subject to conditions set by a parole board. Depending on the jurisdiction, inmates must serve a certain proportion of their sentences before becoming eligible for parole. Upon determination of the parole board, the inmate is granted parole, the conditions of which may require him or her to report regularly to a parole officer, to refrain from criminal conduct, to maintain and support his or her family, to avoid contact with other convicted criminals, to abstain from alcoholic beverages and drugs, to remain within the jurisdiction, and so on. Violations of the conditions of parole may result in revocation of parole, in which case the individual will be returned to prison. The idea behind parole is to allow the offender to be released under community supervision, where rehabilitation and readjustment will be facilitated.[29]

Parolee—An individual released on parole. See Parole.

Participating Entity—An organizational entity that is authorized to access or receive and use entity information and/or databases and resources for lawful purposes through its authorized individual users. This shall include state agencies, contractors, providers (see Provider), or others. In states where applicable, this also includes state health information exchange (HIE) agencies.

[29] Senna, J. J. and Siegel, L. J. (1990). *Introduction to Criminal Justice* (5th ed.). St. Paul, MN: West Publishing Company.

Patient—Refers to any individual who has applied for or been given diagnosis or treatment for medical or behavioral conditions or for substance abuse.

Patient Identifying Information—Per 42 CFR Part 2.11, means the name, address, social security number, fingerprints, photograph, or similar information by which the identity of a patient [who has been tested and treated or has attended a substance abuse program] can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information. The term does not include a number assigned to a patient by a program, if that number does not consist of or contain numbers (such as a social security or driver's license number) which could be used to identify a patient with reasonable accuracy and speed from sources external to the program.

For purposes of this document, the term "protected health information" (PHI) will be used to refer to medical and mental health information, as well as patient identifying information contained in substance abuse testing and treatment records. See Protected Health Information.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, a directory, or a printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Person—Per 45 CFR Part 160 General Administrative Requirements, Subpart A, § 160.103 Definitions, includes entities as well as natural persons.

Personal Data—Personal data refers to any information that relates to an identifiable individual (or data subject). See also Personally Identifiable Information.

Personal Health Information—See Protected Health Information.

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information (PII).

Personally Identifiable Information (PII)—PII is one or more pieces of information that, when considered alone or in the context of how the information is presented or gathered, can contribute to specify (identify) a unique individual. The pieces of information can be personal data, such as biometric characteristics or a unique set of numbers or characters assigned to a specific individual; behavioral data, such as locations or activities; or communications such as innermost thoughts and feelings. Information is personally identifiable even if it carries no explicit and immediately apparent indication of the individual to whom it belongs and even if identification of a unique individual is not contemplated at the time the information is collected or in the use to which it is put. For example, PII includes pictures of a

crowd at a public event, even though no one is yet identified and no one may ever be identified, but it does not include the weather at the event. The fact that the event occurred, if not public information, may also be PII since, if put together with an attendance list, it constitutes PII about behavior.

Personal Representative—A person authorized under state or other law to act on behalf of the individual in making health-related decisions. Examples include a court-appointed guardian with medical authority, a health-care agent under a health-care proxy, and a parent acting on behalf of an unemancipated minor (with exceptions where state law gives minors the right to make health decisions). For a decedent, the personal representative may be an executor, administrator, or other authorized person for matters concerning PHI.

Personnel—Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for an entity, is under the direct control of such entity, whether or not they are paid by the entity.

Pre-trial—Pre-conviction/sentencing supervision in a criminal case by a supervision officer (e.g., pre-trial officer, probation officer) of a defendant in the community as ordered by the court based on the findings of a pre-trial hearing. Pre-trial supervision is typically based on an assessment of the probability the person will attend court hearings and the risk he or she may pose to public safety while the defendant is awaiting further court hearings. Some conditions of supervision may be similar to those of probation and parole. If violated, the defendant likely will be returned to jail while awaiting trial.

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. For purposes of the HIPAA Privacy Rule, privacy means an individual's interest in limiting who has access to personal health-care information. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Notice—A notice describing the practices of the covered entity regarding PHI. Health-care providers and other covered entities must give the notice to patients and research subjects and should obtain signed acknowledgements of receipt. Internal and external uses of PHI are explained. It is the responsibility of the researcher to provide a copy of the Privacy Notice to any subject who has not already received one. If the researcher does provide the notice, the researcher should also obtain the subject's written acknowledgement of receipt.

Note: The HIPAA Privacy Rule expressly excludes inmates from having the right to a Privacy Notice. No current or former inmate has the right to notice of a covered entity's privacy practices.

Privacy Policy—A printed published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the entity will adhere to those legal requirements and entity policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses entity resources wisely and effectively; protects the entity, the individual, and the public; and promotes public trust.

Privacy Protection—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information.

Probation—A sentence entailing the conditional release of a convicted offender into the community under the supervision of the court (in the form of a probation officer) subject to certain conditions for a specified time. The conditions are usually similar to those of parole. (Note: Probation is a sentence, an alternative to incarceration; parole is administrative release from incarceration.) Violation of the conditions of probation may result in revocation of probation.[30]

Probationer—One who is on probation whereby he or she is given some freedom to reenter society subject to the condition that for a specified period, the individual will conduct his or her behavior in a manner approved by a special officer (probation officer) to whom the probationer must report.

Program—As in "federally assisted program" (see Federally Assisted), is defined by 42 CFR Part 2 Subpart A § 2.11, as:

1. An individual or entity (other than a general medical care facility) that holds itself out as providing, and provides, substance abuse diagnosis, treatment, or referral for treatment; or

2. An identified unit within a general medical facility that holds itself out as providing, and provides, substance abuse diagnosis, treatment, or referral for treatment; or

3. Medical personnel or other staff in a general medical care facility whose primary function is the provision of substance abuse diagnosis, treatment, or referral for treatment and who are identified as such

[30] Ibid.

providers. See § 2.12 (e)(1) for examples provided in the regulations.

For example, this definition means that XY Hospital would not be a program but that the Substance Abuse Unit of XY Hospital would be a program because its primary function is providing substance abuse diagnosis and treatment.[31]

Protected Health Information (PHI)—For medical and mental health information, 45 CFR Part 160 General Administrative Requirements, Subpart A, § 160.103 defines PHI as any health information:

1. Except as provided in paragraph 2. of this definition, that is:

   - Transmitted by electronic media;
   - Maintained in electronic media; or
   - Transmitted or maintained in any other form or medium.

   This type of electronic medical information may also be referred to as e-PHI.

2. PHI excludes individually identifiable health information in:

   - Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
   - Records described in 20 U.S.C. 1232g(a)(4)(B)(iv); and
   - Employment records held by a covered entity in its role as employer.

45 CFR Part 164 Subpart C § 164.501 further defines PHI as information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health-care provider, health plan, employer, or health-care clearinghouse; and

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and:

   - That identifies the individual; or
   - With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

The HIPAA Privacy and Security Rules do not protect the individual identifiable health information of persons who have been deceased for more than 50 years. Refer to 45 CFR Part 164 Subpart C § 164.502(f).

The HIPAA Privacy Rule covers PHI in any medium, while the HIPAA Security Rule covers electronic PHI (sometimes referred to as e-PHI).

For substance abuse information, 42 CFR Part 2.1(a) protects "records of the identity, diagnosis, or treatment [or referral for treatment or prevention efforts] of any patient which are maintained in connection with the performance of any substance abuse prevented function."[32]

For purposes of this document, the term "protected health information" (PHI) will be used to refer to medical and mental health information as well as patient identifying information contained in substance abuse testing and treatment records.

Protected Information—Protected information includes personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the [**insert name of state**] Constitution; applicable federal statutes and regulations, such as civil rights laws; applicable state and tribal constitutions; and applicable state, local, and tribal laws and ordinances. Protection may also be extended to organizations by center policy or state, local, or tribal law.

Provider—A community treatment provider that provides medical, mental, and/or substance abuse testing and treatment to individuals released from correctional facilities. Where applicable, providers may or may not have electronic authorized access to PHI contained in the correctional entity's designated record set. Such access to PHI is granted to providers for lawful purposes only.

Psychotherapy notes—Per 45 CFR Part 164 Subpart C § 164.501 Definitions, are defined as notes recorded (in any medium) by a health-care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes

[31] *Information Sharing in Criminal Justice—Mental Health Collaborations: Working with HIPAA and Other Privacy Laws*, John Petrila, J.D., L.L.M, and Hallie Fader-Towe, J.D., Council of State Governments Justice Center, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, www.bja.gov/Publications/CSG_CJMH_Info_Sharing.pdf.

[32] Ibid.

medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

Public—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the entity's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit and without distinction as to the nature or intent of those requesting information from the entity or participating entity.

Public does not include:

- Any employees of the entity or participating entity.
- People or entities, private or governmental, which assist the entity in the operation of the justice information system.
- Public entities whose authority to access information gathered and retained by the entity is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

Qualified Protective Order—Per 45 CFR Part 164 Subpart E § 164.512(e)(1)(v), means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

- Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
- Requires the return to the covered entity or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

Qualified Service Organization (QSO)—Per 42 CFR Part 2, a person or organization that provides services to a 42 CFR Part 2 defined "federally assisted program" (see Program), such as data processing; bill collecting; dosage preparation; laboratory analyses; or legal, medical, accounting, or other professional services; or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy.

Qualified Service Organization Agreement (QSOA)—Per 42 CFR Part 2, a qualified service organization (see definition above) that has entered into a written agreement with a 42 CFR Part 2 program providing drug or alcohol referral, diagnosis, or treatment under which the person or organization acknowledges that in receiving, storing, processing, or otherwise dealing with any records concerning enrolled persons, it is fully bound by these regulations and, if necessary, will resist in judicial proceedings any efforts to obtain access to records of enrolled persons except as permitted by these regulations.

Record—Any item, collection, or grouping of information that includes PII or PHI and is maintained, collected, used, or disseminated by or for the collecting entity or organization.

Redisclosure—Redisclosure is the act of sharing or releasing PHI that was received from another source (e.g., external facility or provider) and made part of a patient's health record or the organization's designated record set.[33]

Redress—Laws, policies, and procedures that address public entity responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the entity's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

Repudiation—The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Research—Means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Retention—Refer to Storage.

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an entity or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Access—A type of access authorization that uses roles to determine access rights and privileges.

[33] AHIMA. "Redisclosure of Patient Health Information (Updated)." Journal of AHIMA 80, no. 2 (February 2009).

A role is a symbolic category of users that share the same security privilege.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Source Entity—Source entity refers to the entity or organizational entity that originates information.

Split Sentence Probation—A split sentence is a form of punishment in which the offender serves up to half of his term of imprisonment outside of prison. In such sentences, while the defendant is ordered to spend compulsory time in jail, he or she is not incarcerated for the entire sentence. The court may suspend part of the offender's sentence and put him or her on probation.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

Storage is frequently used to mean the devices and data connected to the computer through input/output operations; that is, hard-disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This is probably the most common meaning in the IT industry.

In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory, or RAM) and other "built-in" devices, such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

Subcontractor—Per 45 CFR Part 160 General Administrative Requirements, Subpart A, § 160.103 Definitions, means a person to whom a business associate delegates a function, activity, or service the business associate has agreed to perform for a covered entity or business associate. For example, a covered entity may contract with a business associate (contractor), the contractor may delegate to a subcontractor (subcontractor 1) one or more functions, services, or activities the business associate has agreed to perform for the covered entity that require access to PHI, and the subcontractor may in turn delegate to another subcontractor (subcontractor 2) one or more functions, services, or activities it has agreed to perform for the contractor that require access to PHI, and so on. Both the contractor and all of the subcontractors are business associates to the extent they create, receive, maintain, or transmit PHI. See Business Associate.

Substance Abuse—Per 42 U.S.C. § 290dd-2, refers to both alcohol and drug abuse.

Tracking of Disclosures—The HIPAA Privacy Rule gives individuals the right to request an accounting of disclosures of PHI over the previous six years. If an individual authorizes uses or disclosures for research, the disclosures do not need to be tracked, but disclosures must be tracked if the researcher receives an institutional review board-approved waiver of authorization. The accounting of disclosures generally must include: the date of the disclosure, the name of the entity or person (and address if known) who received the PHI, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure. The Rule allows for an alternative tracking option available for research involving 50 or more people.

Treatment—Per 45 CFR Part 164 Subpart C § 164.501 Definitions, is defined as the provision, coordination, or management of health care and related services by one or more health-care providers, including the coordination or management of health care by a health-care provider with a third party; consultation between health care-providers relating to a patient; or the referral of a patient for health care from one health-care provider to another.

Per 42 CFR Part 2 Subpart A § 2.11, treatment is defined as the management and care of a patient suffering from substance abuse, a condition which is identified as having been caused by that abuse, or both, in order to reduce or eliminate the adverse effects upon the patient.

Unsecured Protected Health Information—Means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

User—Entity employee or an individual representing a participating entity who is authorized to access or receive and use an entity's information, databases, and resources for lawful purposes.

Workforce—See Personnel.

Appendix B—Listing of Applicable Federal Laws

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, and tribal (SLT) entities. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution but can (and many do) provide enhanced privacy and other civil liberties protections.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Persons Act.

Federal laws, Executive Orders, regulations, and policies directly affect entities'/agencies' privacy policies. While SLT entities may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., the Health Insurance Portability and Accountability Act [HIPAA]); operation of the Commerce Clause of the U.S. Constitution (e.g., Electronic Communications Privacy Act of 1986); or a binding agreement between a federal agency and an SLT entity (e.g., a memorandum of agreement or memorandum of understanding). When relevant or possibly relevant, entities/agencies are advised to list laws, regulations, and policies within their privacy policies, noting those that may potentially affect the sharing of information.

The development of a protected health information (PHI) privacy policy is primarily designed for entity personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the agency must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an entity's privacy policy, staff and user accountability is greatly diminished, mistakes are made, privacy violations occur, and the public's (and other agencies') confidence in the ability of the entity to protect information is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, information sharing is enhanced.

Following are synopses of primary federal laws that an agency should review and, when appropriate, cite within the policy when developing a PHI privacy policy. The list is arranged in alphabetical order by popular name.

1. **Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget (OMB), Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000**—The Computer Matching and Privacy Act of 1988 (Matching Act) amended the Privacy Act of 1974 to require that data-matching activities or programs of federal agencies that are designed to establish or verify eligibility for federal benefit programs or for recouping payments for debts under covered programs protect personal information. This is accomplished through a computer-matching agreement and publication of a notice in the *Federal Register*. The OMB guidance requires that interagency data sharing provide protection, including provisions for notice, consent (as appropriate), redisclosure limitations, accuracy, security controls, minimization, accountability, and use of Privacy Impact Assessments. Although not directly a requirement of state, local, and tribal (SLT) agencies, the guidance is a useful source of information on the types of protections that should be considered for all interagency data sharing programs.

2. **Confidentiality of Substance Abuse Patient Records, 42 CFR Part 2, Code of Federal Regulations, Title 42: Public Health, Part 2**—42 CFR Part 2 establishes minimum standards to govern the sharing of substance abuse treatment records (patient history information) in programs that are federally assisted. Generally, the sharing of such information is limited to the minimum necessary for the allowed purpose and requires consent of the patient except in specific emergency situations, pursuant to a court order or as otherwise specified. State law should also be consulted to determine whether there are additional limitations or sharing requirements.

3. **Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22**—28 CFR Part 22 is designed to protect the privacy of individuals whose personal information is made available for use in a research or statistical program funded under the Omnibus Crime Control and Safe Streets Act of 1968, the Juvenile Justice and Delinquency Prevention Act of 1974, or the Victim of Crimes Act. The regulation, which may apply to SLT agencies that conduct research or statistical programs, limits the use of such information to research or statistical purposes; limits its revelation to a need-to-know basis; provides for final disposition, transfer, and notice to/consent of data subjects; and identifies sanctions for violations. It provides useful guidance for SLT agencies that wish to make data containing personal information available for research or statistical purposes.

4. **Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601**—This statute authorizes the Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), to support technological advances by states directed at a variety of criminal justice purposes, such as identifying certain categories of offenders, conducting background checks, and determining eligibility for firearms possession. The act defines broad categories of purposes for which funds may be used by OJP and sets forth certain eligibility criteria and assurances and other protocols that must be followed.

5. **Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611**—This statute provides a general overview of the Interstate Identification Index System (IIIS), an information sharing system that contains state and federal criminal history records that are also used for noncriminal justice purposes, such as governmental licensing and employment background checks. Congress recommends the creation of interstate and federal-state agreements to ensure that uniform policies are in place for records exchanges for noncriminal justice purposes and to prevent unauthorized use and disclosure of personal information due to variances in authorized users' policies. This statute is applicable to multijurisdictional information sharing systems that allow **noncriminal justice-related exchanges**.

6. **Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682**—16 CFR Part 682 applies to information systems that maintain or possess consumer information for business purposes. The regulation provides guidance on proper disposal procedures for consumer information records to help protect against unauthorized use or access.

7. **Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681**—The Fair Credit Reporting Act regulates the collection, dissemination, and use of consumer information, including consumer credit information, by consumer reporting agencies. Consumer reporting agencies include specialty agencies, such as agencies that sell information about employment history, **insurance claims**, check-writing histories, **medical records**, and rental history records, as well as credit bureaus. The law primarily deals with the rights of people about whom information has been gathered by consumer reporting agencies and the obligations of the agencies. Government agencies may obtain information from these reporting agencies and should be aware of the nature and limitations of the

information in terms of collection, retention, and error correction.

8. **Family Educational Rights and Privacy Act (FERPA)—**The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.

9. **Federal Civil Rights Laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983**—This is a federal statute that allows an individual to sue public officials in federal court for violations of the individual's civil rights. Civil rights include such things as the Fourth Amendment's prohibitions against unreasonable search and seizure, violations of privacy rights, and violations of the right to freedom of religion, free speech, and free association. It serves as a deterrent to unlawful collection, use, or sharing of information rather than providing specific authority or a prohibition to the collection, use, or sharing of information.

10. **Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301**—This chapter contains the laws governing disposal of records made or received by a federal agency in the normal course of business. It discusses destruction procedures and notices, if required, and the role of the federal archivist. The law applies only to federal agencies, but there may be similar state or local laws applicable to state and local agencies.

11. **Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552**—The federal FOIA, enacted in 1966, provides access to federal agency records or information. It does not, however, allow access to state or local government records. Nearly all states have their own public access statutes that provide access to state- and local-agency records. The interaction of federal and state FOIA laws can create complex issues. Federal statutes, in essence, provide a baseline of legal protections for individuals. While state legislatures may pass laws to supplement these federal guidelines, state laws that interfere with or are contrary to a federal law are preempted. By virtue of the Supremacy Clause of the U.S. Constitution (Article VI, Clause 2), federal law may restrict access to records otherwise available pursuant to a state's FOIA by requiring that certain information be kept confidential. Thus, federal confidentiality requirements may supersede a state FOIA statute mandating public disclosure of a record, but only when there is a specific federal statute (other than the federal FOIA) that mandates the records be kept confidential. In short, records may be available under one FOIA statute but not pursuant to another.

12. **Genetic Information Nondiscrimination Act of 2008 (GINA), Public Law 110-233, 122 Stat. 881—**GINA prohibits discrimination based on an individual's genetic information in both the health coverage and employment contexts. With respect to health coverage, Title I of GINA generally prohibits discrimination in premiums or contributions for group coverage based on genetic information, proscribes the use of genetic information as a basis for determining eligibility or setting premiums in the individual and Medicare supplemental (Medigap) insurance markets, and limits the ability of group health plans, health insurance issuers, and Medigap issuers to collect genetic information or to request or require that individuals undergo genetic testing. Title II of GINA generally prohibits use of genetic information in the employment context, restricts employers and other entities covered by Title II from requesting, requiring, or purchasing genetic information, and strictly limits such entities from disclosing genetic information.

13. **Health Information Technology for Economic and Clinical Health Act (HITECH Act)—**The HITECH Act strengthens the privacy and security protection for individuals' health information. Enacted under Title XIII of the American Recovery and Reinvestment Act of 2009, the HITECH Act set meaningful use of interoperable electronic health records (EHR) adoption in the health-care system as a critical national goal and incentivized EHR adoption. Subtitle D—Privacy, Part 1, Improved Privacy Provisions and Security Provisions, requires HIPAA-covered entities to report data breaches affecting 500 or more individuals to the U.S. Department of Health and Human Services (HHS) and the media, in addition to notifying the affected individuals. This imposes new notification requirements on covered entities, business associates, vendors of personal health records (PHR) and related entities if a breach of unsecured PHI occurs. Subtitle D also extends the complete Privacy and Security Provisions of HIPAA to business associates of covered entities. This includes the extension of newly updated civil and criminal penalties to business associates. These changes are also required to be included in any business associate agreements with covered entities.

14. **Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191**—HIPAA was enacted to improve the Medicare and Medicaid programs and the efficiency and effectiveness of the nation's

health-care system by encouraging the development of a national health information system through the establishment of standards and requirements for the electronic transmission of health information. To that end, Congress directed the U.S. Department of Health and Human Services (HHS) to issue safeguards to protect the security and confidentiality of health information. To implement HIPAA's privacy requirements, HHS promulgated regulations setting national privacy standards for health information: the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule")—42 U.S.C. § 1320d-2; 45 CFR Parts 160, 164 (2003).

15. **HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, Code of Federal Regulations, Title 45, Parts 160 and 164**—This "Privacy Rule" sets forth national standards for the privacy and security of individually identifiable health information (45 CFR Part 164, Subpart E (2003)). This rule has been described as providing a "federal floor" of safeguards to protect the confidentiality of medical information. State laws that provide stronger privacy protection will continue to apply over and above the federal privacy protection. The general rule under these standards states that a covered entity may not use or disclose PHI except as permitted or required by the rules (45 CFR Part 164.502(a) and § 164.103 [defining PHI and use]). The Privacy Rule applies to the following covered entities: (1) a health plan, (2) a health-care clearinghouse, and (3) a health-care provider who transmits any health information in electronic form in connection with certain transactions (42 U.S.C. § 1320d-1(a) (2003); 45 CFR Part 160.102 (2003)). Since the Privacy Rule applies only to a covered entity, a governmental body begins its inquiry by first determining whether it is a covered entity under the Privacy Rule (45 CFR Part 160.103 (2003) [defining health plan, health-care clearinghouse, health-care provider]). If it is a covered entity, it then looks to the Privacy Rule for a permitted or required disclosure.

16. **Indian Civil Rights Act of 1968, 25 U.S.C. § 1301 et seq., United States Code, Title 25, Chapter 15, Subchapter I**—This act contains definitions of relevant terms and extends certain constitutional rights to Indian tribes exercising powers of self-government.

17. **National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490**—In each state, an authorized criminal justice agency of the state shall report child abuse crime information to or index child abuse crime information in the national criminal history background check system. A criminal justice agency can satisfy the requirement by reporting or indexing all felony and serious misdemeanor arrests and dispositions. The U.S. Attorney General (AG) is required to publish an annual statistical summary of child abuse crimes. The act requires that 80 percent of final dispositions be entered in the state databases by December 1998, with steps being taken toward 100 percent entry.

    A 1994 amendment required that the AG—in consultation with federal, state, and local officials, including officials responsible for criminal history record systems, and representatives of public and private care organizations and health, legal, and social welfare organizations—shall develop guidelines for the adoption of appropriate safeguards by care providers and by the state for protecting children, the elderly, and individuals with disabilities from abuse.

18. **National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616**—The compact establishes an infrastructure by which states can **exchange criminal records for noncriminal justice purposes** according to the laws of the requesting state and provide reciprocity among the states to share records without charging each other for the information. The Compact Council, as a national independent authority, works in partnership with criminal history record custodians, end users, and policymakers to regulate and facilitate the sharing of complete, accurate, and timely criminal history record information to noncriminal justice users in order to enhance public safety, welfare, and the security of society while recognizing the importance of individual privacy rights.

19. **Patient Safety and Quality Improvement Act of 2005, 42 U.S.C., Chapter 6A, Subchapter VII, Part C – Patient Safety Improvement § 299(b)**—The Patient Safety and Quality Improvement Act of 2005 (PSQIA) establishes a voluntary reporting system designed to enhance the data available to assess and resolve patient safety and health-care quality issues. To encourage the reporting and analysis of medical errors, Section 922 provides federal privilege and confidentiality protections for patient safety information, called patient safety work product. Section 922 provides for how patient safety work product may be disclosed. PSQIA authorizes the U.S. Department of Health and Human Services to impose civil money penalties for violations of patient safety confidentiality. PSQIA also authorizes the Agency for Healthcare Research and Quality (AHRQ) to list patient safety organizations (PSOs). PSOs are the external experts that collect and review patient safety information.

20. **Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a**—This section of the Privacy Act prohibits the release of records from a record system without the expressed consent of the individual to whom the record pertains. This

provision does not apply to court orders for records or when a written request is made by the head of a government agency tasked with civil or criminal law. Additionally, the head of any agency can promulgate rules to exempt a system of records if it is maintained by an agency whose principal function is to enforce criminal laws and if the information is compiled for the purpose of a criminal identification, investigation, or any other stage of the criminal process.

21. **Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)**—This memorandum provides a security checklist from the National Institute of Standards and Technology (NIST) to protect remote information removed from or accessed from outside an agency's physical location specific to personally identifiable information (PII). The NIST checklist requires that agencies verify PII in need of protection, confirm the adequacy of organization policy surrounding PII protection, and implement any necessary protections for PII transported or stored off-site or accessed remotely. In addition to the NIST checklist, the memorandum recommends implementing data encryption on all mobile devices, allowing remote access only with two-factor authentication, using timeout functions on devices, and logging all computer-readable data extracts from databases with sensitive information, while verifying each extract has either been erased within 90 days or its use is still required.

22. **Safeguarding Against and Responding to the Breach of Personally Identifiable Information, OMB Memorandum M-07-16 (May 2007)**—This memorandum applies to federal agency-held information and information systems, requiring development and implementation of a breach notification policy applicable to personally identifiable information in the possession of the agency. Development of a breach notification policy includes a review of existing privacy and security requirements, development of requirements for incident reporting and handling, and procedures for internal and external notification. SLT agencies that are not subject to an existing breach notification law or policy may use the federal requirements as a template for developing their own breach notification policy.

23. **U.S. Constitution, First, Fourth, and Sixth Amendments**—The First, Fourth, and Sixth Amendments to the U.S. Constitution and, indeed, the entire Bill of Rights establish minimum standards for the protection of the civil rights and civil liberties of Americans. The First Amendment protects religious freedom, speech, the press, the right to peaceably assemble, and the right to petition the government for a redress of grievances. The Fourth Amendment protects the people from unreasonable searches and seizures and requires that warrants be issued only upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the person or things to be seized. The Sixth Amendment establishes the right of an accused individual to a speedy and public trial by an impartial jury, to be informed of the nature and cause of the charges, to confront witnesses, to have compulsory process to obtain witnesses, and to have the assistance of legal counsel.

Appendix C—Release of Information: Consent Authorization Guidance

Obtaining permission from an individual to release his or her PHI or patient identifying information is a straightforward way to facilitate information sharing. Both HIPAA and 42 CFR Part 2, however, have specific requirements regarding the elements (see section B. within this appendix) that must be included in consent authorizations. For example, in addition to form requirements, entities must:

- Inform individuals of their right to revoke authorizations,
- Ensure that the writing be in plain language,
- Provide a copy of the signed authorization to the individuals, and
- Document and retain any signed authorization.

Additionally, when entities obtain or receive valid authorizations, the use or disclosure of PHI or patient identifying information must be consistent with the authorization. Finally, entities are also encouraged to explain to the individual the purpose and benefits for providing his or her consent to disclose the requested types of information.

A. Do you need an authorization to release PHI or patient identifying information?

As a general rule, when entities are in doubt about whether they need to obtain an individual's authorization, it is best to err on the side of caution and obtain a signed release and to maintain records and documentation of all releases obtained by the entity. While HIPAA and 42 CFR Part 2 mandate that entities or programs obtain authorizations, corrections entities also are guided to refer to their state laws for state-specific requirements for the release of PHI and patient identifying information.

The following scenarios describe conditions by which an authorization may or may not be required in accordance with HIPAA and 42 CFR Part 2.

1. Corrections entity needs to receive PHI or patient identifying information

a. HIPAA and Corrections Receiving PHI

In accordance with HIPAA's 45 CFR Part 164 Subpart C § 164.512(k)(5), corrections entities that need to receive PHI in order to complete an assessment or provide medical care, counseling, or treatment for an individual who is **under lawful custody by the entity** may receive PHI from HIPAA-covered entities without obtaining an individual release-of-information consent authorization.

b. 42 CFR Part 2 and Corrections Receiving Patient Identifying Information

Per 42 CFR Part 2, the corrections entity would need to obtain a signed consent authorization in order to receive the patient identifying information from the provider.

2. Corrections entity needing to share PHI or patient identifying information (for released individuals)

a. HIPAA and Corrections Sharing PHI

Under HIPAA, once an individual is released from lawful custody, that individual's rights are restored regarding the need to obtain his or her permission to share PHI. In this situation, whether a HIPAA-covered entity or not, the corrections entity that provided medical care and/or treatment to the individual while under custody will need to obtain the individual's permission to release his or her PHI. For example, a corrections entity that provided counseling services to an inmate while incarcerated would need to obtain a signed consent authorization once the individual was released in order to share the PHI with a community health or behavioral health provider for follow-up services.

b. 42 CFR Part 2 and Corrections Sharing Patient Identifying Information

Per 42 CFR Part 2, a consent authorization would also be required to share patient identifying information.

3. Probation/parole needing to receive PHI or patient identifying information from community health or behavioral health providers

a. HIPAA and Probation/Parole

Under HIPAA, individuals who are released from custody but who are under supervision, such as on probation or parole, will need to provide a signed consent authorization in order to allow the probation/parole officers to receive status reports or updates from community health or behavioral health providers regarding the individuals' progress or attendance at certain rehabilitation, counseling, or treatment programs. However, the consent authorization may not be required if a court order stipulates that the PHI or patient identifying information is to be shared with a probation/parole officer as part of the requirements or conditions for the probation/parole. Refer to Appendix E for sample court order language.

b. 42 CFR Part 2 and Probation/Parole

42 CFR Part 2 Subpart C § 2.35 states that a program may disclose information about a patient to those persons within the criminal justice system who may have made participation in the program a condition of the disposition of any criminal proceedings against the patient or of the patient's parole or other release from custody if:

- The disclosure is made only to those individuals within the criminal justice system who have a need for the information in connection with their duty to monitor the patient's progress (e.g., a prosecuting attorney who is withholding charges against the patient, a court granting pre-trial or post-trial release, probation or parole officers responsible for supervision of the patient); **and**

- The patient has signed a written consent meeting the requirements of § 2.31 (form of written consent, except (a)(8) regarding revocation) and also stating a reasonable period during which it remains in effect, taking into consideration the anticipated length of treatment, type of criminal proceeding involved, and need for information in connection with the final disposition of that proceeding and when the final disposition will occur, and other pertinent factors.

  The written consent must state that it is revocable upon the passage of a specified amount of time or the occurrence of a specified, ascertainable event and may be no later than the final disposition of the conditional release or other action in connection with which consent was given.

B. Requirements for Consent Authorization Forms

Both HIPAA and 42 CFR Part 2 require similar core elements and notice statements that must be included in valid consent-to-release authorization forms. For more information on these regulations' form requirements, refer to sections B.1. and B.2. Included within this appendix is a basic consent-to-release authorization form that entities may customize to ensure that both regulations' requirements are met.

1. HIPAA Requirements

a. Elements

In accordance with HIPAA's 45 CFR Part 164 Subpart C § 164.508(c), Core elements and requirements, a valid authorization must contain at least the following elements:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- The name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure.
- The name or other specific identification of the person(s) or class of persons to whom the covered entity may make the requested use or disclosure.
- A description of each purpose of the requested use or disclosure. **Note:** The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. **Note:** The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository.
- Signature of the individual and date. **Note:** If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual also must be provided.

b. Notice Statements

In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

- The individual's right to revoke the authorization in writing, and either:
    - The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
    - To the extent that the exceptions to the right to revoke are included in the notice required by HIPAA's notice of privacy practices for PHI, as per § 164.520, a reference to the covered entity's notice.
- The ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization, by stating either:
    - The covered entity may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or
    - The consequences to the individual of a refusal to sign the authorization when the covered entity can, per § 164.508(b)(4), condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
- The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer to be protected.

2. 42 CFR Part 2 Requirements

a. Elements

In accordance with 42 CFR Part 2 § 2.31 Form of written consent, a written consent to a disclosure under these regulations must include:

- The specific name or general designation of the program or person permitted to make the disclosure.

- The name or title of the individual or the name of the organization to which disclosure is to be made. Note: The authorization has to specifically state the name of the provider **or** the general designation of the treatment center (e.g., Shady Grove Substance Abuse Center).

- The name of the patient.

- The purpose of the disclosure.

- How much and what kind of information is to be disclosed.

- The signature of the patient and, when required for a patient who is a minor, the signature of a person authorized to give consent under § 2.14; or, when required for a patient who is incompetent or deceased, the signature of a person authorized to sign under § 2.15 in lieu of the patient.

- The date on which the consent is signed.

- The date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must ensure that the consent will last no longer than reasonably necessary to serve the purpose for which it is given.

In the case of minors, in accordance with 42 CFR § 2.14, providers must **always** obtain the minor's consent before the provider can gain access to the minor's 42 CFR Part 2 record. Depending on state law, the provider might need to obtain the parent's or guardian's consent as well. In other words, if a state law gives a minor the legal authority to consent to treatment on his or her own, without a parent's or guardian's permission or knowledge, then only the minor's consent is required to disclose the minor's information. If state law requires parental consent for the minor to be provided alcohol or drug treatment, then the consent of **both** the minor patient and the parent or guardian is required for disclosures. The minor's written consent must be obtained first in all cases.

b. Notice Statements

In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

- A statement that the consent is subject to revocation at any time, except to the extent that the program or person making the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third-party payer.

- Under 42 CFR Part 2, a single consent form can authorize a disclosure of information about a patient to one recipient, and simultaneously authorize that recipient to redisclose that information to any additional entity or entities (such as other affiliated health-care providers identified in the consent form), provided that the purpose for the disclosure is the same. The following required statement prohibiting redisclosure must accompany the information disclosed through consent, so that each subsequent recipient of that information is notified of the prohibitions on redisclosure.

> ***This notice covers the disclosure of information to you concerning a client in alcohol/drug treatment, made to you with the consent of such client. This information has been disclosed to you from records protected by federal confidentiality rules (42 C.F.R. Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any substance abuse patient.***

3. Other Optional Elements for Consideration

The Association of State Correctional Administrators (ASCA) partnered with the American Probation and Parole Association (APPA) to conduct a survey of both organizations' membership concerning privacy practices and policies within correctional agencies (community and institutional)—titled "Survey Of Correctional Privacy Practice & Policies." A total of 104 individuals recorded responses to the survey. Many of these individuals provided samples of their authorization forms. In addition to the core elements required for consent authorizations by HIPAA and 42 CFR Part 2, the following is a list of optional elements that entities participating in the ASCA/APPA survey used in their authorization forms. Entities are encouraged to consider adding any of these that may apply and that would enhance the understandability and use of an entity-developed consent authorization form.

a. Patient Information

According to best practices used to confirm the identity of an individual, the following fields are recommended for matching records for identification purposes:

- ZIP code
- Last four digits of the social security number

Other optional identifying information you may want to consider requesting:

- ID number(s) (e.g., full SSN, state identifying number [SIN/SID], inmate ID, case number)
- Last known street address
- City
- State
- Last known home phone number
- Last known cell phone number, if different
- Alias(es)
- Guardian/parent, for minors or conservator/legal representative
- Mother's maiden name
- Father's name
- School (current or last attended)
- Place of birth

b. Information-Providing Agency

It may be helpful for entities to develop a checklist of known providers to allow the individual to select providers from which he or she received services. This list of individuals/agencies granted permission to share can include the individual's/agency's phone number, e-mail address, street address, and also a place for the patient to complete any comments associated with the information from this provider. The provider list may be further categorized by type, such as physician, counselor/psychologist/psychiatrist, etc.

c. Information-Receiving Agency

It may be helpful for entities to develop a checklist of individuals/agencies allowed to receive information. This information will be shared only with individuals responsible for this case. The recipient list, as with the provider list, may be further categorized by type, such as correctional agency(ies), etc. Following is other optional information you may want to consider providing:

1. Case manager
2. Individual officer(s) (probation/parole)
3. Phone number
4. Fax number
5. Street address
6. City
7. State
8. ZIP code

d. Type of Information to Be Shared

Each consent, per the regulations cited earlier, **must** indicate the type and amount of information being authorized for release. For ease of the individual completing the authorization, it may be helpful to provide a prepopulated list of types of information requested, which allows the individual to select each that applies, such as:

- **Substance abuse and treatment information**
- **Mental health and treatment information**
- **Medical and dental history and treatment information**

Note: HIV and STD information, per state law, may require a separate authorization. Entities are encouraged to become familiar with their states' laws regarding these types of information.

Following are other optional types of information you may want to consider requesting consent for disclosure. While some of these may be requested by jails or correctional institutions, others may be requested by pre-trial/probation/parole. Entities will need to refer to state law and policy to determine what types of information require a consent authorization. Information that does not require consent should not be included on a consent form. Note: For juvenile records, refer to state law and policy for release requirements.

1. Academic and educational information (Entities will need to refer to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, to ensure that authorizations meet FERPA requirements.[34] For example, FERPA requires the consent to include the following fields: records to be disclosed, purpose of the use of the information, the classified parties to whom disclosure is to be made, date of signature, student signature, and signature of the custodian of the record.)
2. Supervision data and probation/parole reports/records
3. Program completion and compliance (e.g., vocational, domestic violence/anger management, parenting)
4. Program or treatment progress updates/reports
5. Program or treatment discharge plan/completion letter
6. Testing results and treatment (e.g., developmental disabilities, cognitive behavioral programming)
7. Treatment plans (e.g., treatment plans for sexual offenders)
8. Results of drug/alcohol tests

[34] www.gpo.gov/fdsys/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20-chap31-subchapIII-part4-sec1232g.pdf.

9. Employment records

e. Purpose and Expected Use of the Information

Each consent, according to the regulations cited earlier, **must** state the purpose for which the information is being requested. The following is a nonexhaustive list of potential reasons an entity may prepopulate on the consent form to enable the individual to specify the purpose for requesting information to be released.

1. Inmate classification
2. Coordinate treatment with family and/or concerned others
3. Enable supportive activity with employer
4. Effectively work with person(s) in the legal system to understand and support treatment
5. Obtain insurance, employment benefits
6. Obtain Medicare, Medicaid, insurance premium subsidies, and/or medical cost sharing reduction assistance
7. Probation/parole supervision
8. Court-ordered investigation
9. Referral to program/placement
10. Individual evaluation and treatment
11. Attendance/lack of attendance at treatment sessions
12. Cooperation with treatment program
13. Diagnosis
14. Prognosis
15. Program monitoring/completion
16. Discharge/release planning
17. Research, evaluation, and audit

C. Defective Authorizations

1. HIPAA Defective Authorizations

In accordance with HIPAA's 45 CFR Part 164 Subpart C § 164.508(b)(2), an authorization is not valid if the document submitted has any of the following defects:

- The expiration date has passed or the expiration event is known by the covered entity to have occurred.
- The authorization has not been filled out completely, with respect to required elements.
- The authorization is known by the covered entity to have been revoked.
- The authorization violates rules regarding compound authorizations (combined authorizations, as described in 1. below) or conditioned authorizations (conditioning the provision of treatment, payment, enrollment, or benefit eligibility on the authorization, as described in 2. below).
- Any material information in the authorization is known by the covered entity to be false.

a. Compound Authorizations

In accordance with HIPAA's 45 CFR Part 164 Subpart C § 164.508(b)(3), an authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except as follows:

- An authorization for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of PHI for such research or a consent to participate in such research.

- An authorization for a use or disclosure of psychotherapy notes may be combined only with another authorization for a use or disclosure of psychotherapy notes.

- An authorization, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits (as described in b. below).

In accordance with § 164.508(b)(3)(i) and (ii), covered entities are permitted to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. These provisions allow covered entities to combine authorizations for the use and disclosure of PHI for clinical trials and related biospecimen banking activities, as well as other scenarios that often occur in research studies.

b. Prohibition on Conditioning of Authorizations

In accordance with HIPAA's 45 CFR Part 164 Subpart C § 164.508(b)(4), a covered entity may not condition the provision to an individual of treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of authorization, except:

- A covered health-care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of PHI for such research (as described in C.1. above);

- A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

    - The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk-rating determinations (see Underwriting Note, below); and

    - The authorization is not for a use or disclosure of psychotherapy notes.

A covered entity may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party.
Underwriting Note: Per the Genetic Information Nondiscrimination Act of 2008 (GINA), Public Law 110-233, 122 Stat. 881, and § 164.502(a)(1)(iv), an authorization cannot be used to permit a use or disclosure of genetic information for underwriting purposes. Further, GINA generally prohibits discrimination in premiums or contributions for group coverage based on genetic information, proscribes the use of genetic information as a basis for determining eligibility or setting premiums in the individual and Medicare supplemental (Medigap) insurance markets, and limits the ability of group health plans, health insurance issuers, and Medigap issuers to collect genetic information or to request or require that individuals undergo genetic testing. Genetic information is health information, and health plans, health insurance issuers (including HMOs), and issuers of Medicare supplemental policies are prohibited from using or disclosing genetic information for underwriting purposes.

2. **42 CFR Part 2 Defective Authorizations**

In accordance with 42 CFR Part 2, a disclosure may not be made on the basis of a consent which:

- Has expired.

- On its face, substantially fails to conform to any of the requirements set forth in this regulation.

- Is known to have been revoked.

- Is known, or through a reasonable effort could be known, by the person holding the records to be materially false.

D. Revocation of Authorizations

In accordance with HIPAA's 45 CFR Part 164 Subpart C § 164.508(b)(5), an individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

- The covered entity has taken action in reliance thereon; or

- If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

In accordance with 42 CFR Part § 2.31, the consent must include "the date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must insure that the consent will last no longer than reasonably necessary to serve the purpose for which it is given."

In accordance with 42 CFR Part § 2.35, disclosures to elements of the criminal justice system which have referred patients, "Revocation of consent, the written consent must state that it is revocable upon the passage of a specified amount of time or the occurrence of a specified, ascertainable event. The time or occurrence upon which consent becomes revocable may be no later than the final disposition of the conditional release or other action in connection with which consent was given."

Consent-to-Release Information Authorization		
A. PATIENT INFORMATION		
Patient's Full Name		**Date of Birth (M/D/YR)**
Street Address	**Medical Record Number**	**Social Security Number**
City, State, ZIP	**Inmate ID Number**	**Telephone Number**
I hereby authorize the use or disclosure of my individually identifiable protected health information as indicated.		
B. DISCLOSED FROM—Person(s)/organization(s) authorized to provide information.	**C. DISCLOSED TO—Person(s) or organization(s) authorized to receive the information.**	

D. INFORMATION AUTHORIZED TO BE RELEASED	
Check all that apply	***For the following dates of service (if known):***
Medical Health Information	
o Medical history and physical condition	
o Medical progress notes	
o Treatment plan/physician orders	
o Lab results/reports (excluding HIV testing)	
o X-rays and diagnostic test results	
o Medication records	
o Allergies	
o Diabetes	
o Disabilities	
o Activity restrictions	
o Tuberculosis information/status	
o Other communicable disease(s)	
o Other medical information:	

HIV/AIDS, Mental Health/Psychological, and Substance Use Information
If records include HIV/AIDS, mental health/psychological, or substance use information, a signature is required for each authorized disclosure.

Information to Disclose (Check all that apply.)	**For the following dates of service** (if known)	**Signature***
HIV/AIDS Information		
o HIV test/AIDS-related information/status		
Mental Health/Psychological Information		
o All mental and behavioral health information		
o Diagnosis/treatment plans (including medication)		
o Intake/termination statements		
o Type of professional services rendered (psychotherapy, psychiatric)		
o Dates on which services were performed		

o Psychological testing		
Information to Disclose (Check all that apply.)	**For the following dates of service** (if known)	**Signature***
Mental Health/Psychological Information, *Continued*		
o Psychiatric examinations		
o Psycho***social*** assessments		
o Psychiatric records		
o Suicide watch records		
o Sex offender treatment		
o Mental health progress notes		
o Other mental health information:		
Substance Use Testing and Treatment Information		
o Alcohol/substance use/addiction treatment records		
o Results of substance testing		
o All substance abuse treatment progress notes		
o Other alcohol/substance use/addiction information:		

E. PURPOSE FOR DISCLOSURE(S)

This protected health information is being used or disclosed for the following purposes:

F. EXPIRATION OF AUTHORIZATION

This authorization begins on _____ (Date)

Expiration:

o **Option1:** This authorization expires on the first of the following, shown below:

o **Option 2: This authorization expires on the following event, condition, or exact date (whichever comes first) as shown below:**

Event: _____

Condition: _____

Exact Date: _____

Examples

Event = For example, a judge terminates the individual's placement in a program or the individual is otherwise removed from the program.

Condition = For example, the individual successfully pays all fines, fees, and restitution.

Exact Date = For example, stating "Three years from the date the individual was assigned to the program."

G. PATIENT NOTICES	
Initials*	**You must initial that you have read and understand each of the following patient notices.**
	1. Redisclosure of Medical Information: I understand that the information used or disclosed may be subject to redisclosure by the person(s) or organization(s) authorized to receive it, and would then no longer be protected by federal privacy regulations. The Department of Corrections is not responsible for unauthorized redisclosure by the designated recipient.
	2. Confidentiality of Substance Abuse Information: I understand that if I authorize the release of substance abuse information (as authorized on this form), this information will be disclosed from records protected by federal law and regulations relating to "confidentiality of substance abuse patient records," (42 CFR Part 2, 42 U.S.C. § 290dd-2). The federal rules prohibit the entity, which I have designated to receive this alcohol and/or substance abuse information, from making any further disclosure of this information unless further disclosure is expressly permitted by my written consent or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any substance abuse patient.
	3. Right to Refuse: I understand that this authorization is voluntary and that I may refuse to sign this authorization. I understand that refusal to sign this form may disqualify me from becoming eligible for supervision by [**insert name of community corrections program**]. I further understand that my refusal to sign will not affect my ability to obtain treatment or payment or affect my eligibility for benefits, unless the treatment is research related.
	4. Right to Revoke (only if not in court-ordered treatment): I understand that, as part of voluntary treatment, I have the right to revoke this authorization in writing at any time by sending written notification to **[insert name of privacy contact]** at **[insert mailing address]**. However, I understand that any action already taken in reliance on this authorization cannot be reversed, and my revocation will not affect those actions. I further understand that such action may result in my termination from [**insert name of community corrections program**].
	5. Right to Inspect/Copy: I understand that I may obtain a copy of the protected health information to be used or disclosed under this authorization upon my release from [**insert name of community corrections program**].
	6. Fees for copies: Federal and state laws permit a reasonable cost-based fee to be charged for the copying of patient records (which may include cost of supplies, postage, and labor costs for making copies, whether in paper or electronic form). I may be required to pre-pay for copies (or have the cost billed to my inmate account); if not, then my copies may be mailed along with an invoice for copying fees.

H. SIGNATURES		
THIS FORM MUST BE FULLY COMPLETED BEFORE SIGNING ***Note that multiple signatures and initials are required.**		
***Signature of Individual** *Person about whom the information relates*	***Signature of Guardian or Patient's Personal Representative**	**Description of Authority (or Relationship) to Act for the Individual**
Date:	**Date:**	

A copy of this completed, signed, and dated form must be given to the Individual or other signatory.

Official Use Only		
Date Received	**Processed By**	**Log #**

Attention Recipient Entity—Prohibition on Redisclosure of Confidential Information

This notice covers the disclosure of information to you concerning a client in alcohol/drug treatment, made to you with the consent of such client. This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any substance abuse patient.

Appendix D—Contractual Agreements

Pursuant to both HIPAA and 42 CFR Part 2, entities can disclose PHI, without individual consent, to outside organizations that perform certain functions or provide services to the entity or on behalf of the entity, by establishing contractual agreements. HIPAA calls these outside organizations "business associates" and their contractual agreements "Business Associate Agreements"—or BAAs. 42 CFR Part 2 calls these organizations "qualified service organizations" and their contractual agreements "Qualified Service Organization Agreements"—or QSOAs. BAAs and QSOAs, while very similar in contractual requirements, each have their own set of criteria for what constitutes a business associate or a qualified service organization and the conditions and purposes by which a contractual agreement can be established.

A. HIPAA Business Associate[35]

By law, the HIPAA Privacy Rule applies only to covered entities (health plans, health-care clearinghouses, and certain health-care providers). However, most health-care providers and health plans do not carry out all of their health-care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. HIPAA's Privacy Rule allows covered entities to disclose PHI to these "business associates" if the providers or plans obtain satisfactory assurances[36] that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the HIPAA Privacy Rule. Covered entities may disclose PHI to an entity in its role as a business associate ***only*** to help the covered entity carry out its health-care functions but **not** for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

HIPAA requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

What Is a "Business Associate?" A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI **on behalf of or provides services to** a covered entity. While a member of the covered entity's workforce is not a business associate, a covered health-care provider, health plan, or health-care clearinghouse can be a business associate of another covered entity.

HIPAA lists some of the functions or activities as well as the particular services that make a person or entity a business associate, if the activity or service involves the use or disclosure of PHI. These include payment or health-care operations activities as well as other functions or activities regulated by the Administrative Simplification Rules.

- Business associate ***functions*** and activities include claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing.

[35] HHS, Health Information Privacy, Understanding HIPAA, For Covered Entities and Business Associates, Business Associates, www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.
[36] § 164.502(e)(1).

- Business associate ***services*** are as follows: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial.

.

According to § 160.103, a business associate **does not include**:

- **A health-care provider, with respect to disclosures by a covered entity to the health-care provider concerning the treatment of the individual.**
- A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.
- A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
- A covered entity participating in an organized health-care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health-care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health-care arrangement by virtue of such activities or services.

For a more detailed definition of "business associate," refer to Appendix A, Glossary of Terms and Definitions.

B. HIPAA Business Associate Agreements (BAAs)

If a covered entity engages a business associate to help it carry out its health-care activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with HIPAA's requirements to protect the privacy and security of PHI. In addition to these contractual obligations, business associates are directly liable for compliance with certain HIPAA provisions.[37]

It is important to note that for covered entities, such as corrections entities that meet HIPAA's definition of a covered entity (or the medical component of a correctional facility where the component is a covered entity), which engage the services of health-care providers (who are also covered entities), HIPAA explicitly excludes from the business associate requirements disclosures by a covered entity to a health-care provider for treatment purposes. See 45 CFR 164.502(e)(1). ***Therefore, any covered health-care provider (or other covered entity) may share PHI with a health-care provider for treatment purposes without a business associate contract.*** However, this exception does not preclude one health-care provider from establishing a business associate relationship with another health-care provider for some ***other*** purpose.[38]

1. BAA Requirements

As mentioned earlier, a covered entity may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.[39] In addition, § 164.502(b) states that when using or disclosing PHI or when requesting PHI from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit PHI to the **minimum necessary** to accomplish the intended purpose of the use, disclosure, or request.

The HIPAA Privacy Rule does not "pass through" its requirements to business associates or otherwise cause business associates to comply with the terms of the Rule. The assurances that covered entities must obtain prior to disclosing protected health information to business associates create a set of contractual obligations far narrower than the provisions of the Rule, to protect information generally and help the covered entity comply with its obligations under the Rule.[40]

Business associates, however, are not subject to the requirements of the Privacy Rule, and the Secretary cannot

[37] U.S. Department of Health and Human Services (HHS), Health Information Privacy for Covered Entities and Business Associates, www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html.
[38] HHS, Health Information Privacy, "When is a health care provider a business associate of another health care provider?," www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/240.html.
[39] www.gpo.gov/fdsys/pkg/CFR-2002-title45-vol1/xml/CFR-2002-title45-vol1-sec164-502.xml.
[40] HHS, Health Information Privacy, FAQs, "Has the Secretary exceeded the HIPAA statutory by requiring 'business associates' to comply with the Privacy Rule, even if that requirement is through a contract?," www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/233.html.

impose civil monetary penalties on a business associate for breach of its business associate contract with the covered entity, unless the business associate is itself a covered entity. For example, covered entities do not need to ask their business associates to agree to appoint a privacy officer or develop policies and procedures for use and disclosure of protected health information.[41]

A covered entity's contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). For example, the contract must (1) describe the permitted and required uses of protected health information by the business associate, (2) provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law, and (3) require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract. Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).[42]

Further, in 2013 HIPAA added a requirement that business associates comply with the security administrative, physical, and technical safeguards requirements in 45 CFR Part 164 Subpart C §§ 164.306, 164.308, 164.310, and 164.312, as well as with the HIPAA Security Rule's policies and procedures and documentation requirements in § 164.316 in the same manner as these requirements apply to covered entities, and that business associates are civilly and criminally liable for violations of these provisions, per the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Subtitle D-Privacy, PART 1—Improved Privacy Provisions and Security Provisions, Section 13401.

HIPAA's recommended sample contract provisions are included in this appendix on the next page. However, a sample contract that complies with both HIPAA (for medical and mental health information) and 42 CFR Part 2 (for substance abuse information) is provided later within this appendix to use as a starting point to develop a federally compliant contract between the entity/program and a business associate/qualified service organization.

For a list of Frequently Asked Questions (FAQs) on BAAs, refer to the HHS Web site at www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/index.html.

2. **HIPAA's Sample Business Associate Contract Provisions**[43]

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has published the following sample contract language (67 Federal Register 53264, August 14, 2002) for inclusion in a BAA. These provisions are designed to help covered entities more easily comply with the BAA requirements of the HIPAA Privacy Rule. However, **use of these sample provisions is not required for compliance with the Privacy Rule**. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities, or they may be incorporated into a separate business associate agreement. Note: These provisions address only concepts and requirements set forth in the HIPAA Privacy Rule and alone are not sufficient to result in a binding contract under state law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for compliance with state law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Further, a covered entity may want to include other provisions that are related to the HIPAA Privacy Rule but that are not required by it. For example, a covered entity may want to add provisions in a BAA in order for the entity to be able to rely on the business associate to help the covered entity meet its obligations under the HIPAA Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically

[41] Ibid.

[42] HHS, Health Information Privacy, Understanding HIPAA, For Covered Entities and Business Associates, Business Associates, www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.

[43] This version of Sample Business Associate Contract Provisions was revised on June 12, 2006, to amend the regulatory cites to the following terms: "individual," "protected health information," and "required by law." Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.

addressed in these sample provisions; for example, having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.
A sample contract that complies with both HIPAA (for medical and mental health information) and 42 CFR Part 2 (for substance abuse information) is provided later within this appendix to use as a starting point to develop a federally compliant contract between the entity/program and a business associate/qualified service organization.

HIPAA's Sample Business Associate Contract Provisions

Definitions: Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Privacy Rule.

Examples of specific definitions:

a. Business Associate. "Business Associate" shall mean [**insert name of business associate**].

b. Covered Entity. "Covered Entity" shall mean [**insert name of covered entity**].

c. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

d. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

e. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

f. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

g. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

a. Business Associate agrees to not use or disclose PHI other than as permitted or required by the Agreement or as Required by Law.

b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement.

c. Business Associate agrees to comply with the security administrative, physical, and technical safeguards requirements in 45 CFR Part 164 Subpart C §§ 164.306, 164.308, 164.310, and 164.312, as well as with the HIPAA Security Rule's policies and procedures and documentation requirements in § 164.316 in the same manner as these requirements apply to covered entities, and agrees that business associates are civilly and criminally liable for violations of these provisions, per the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Subtitle D-Privacy, PART 1—Improved Privacy Provisions and Security Provisions, Section 13401.

d. In accordance with 45 CFR Part 164 Subpart D § 164.410(a), business associates shall, following the discovery of a breach of unsecured PHI, notify [**name of covered entity**] of such breach without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The notification will be made in the manner specified by the U.S. Department of Health and Human Services (HHS) Web site.

e. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]

f. Business Associate agrees to report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware.

g. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of, the Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

h. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [**insert negotiated terms**], to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. [Not necessary if Business Associate does not have PHI in a Designated Record Set.]

i. Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and in the time and manner [**insert negotiated terms**]. [Not necessary if Business Associate does not have PHI in a Designated Record Set.]

j. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available [**to the Covered Entity, or**] to the Secretary, in a time and manner [**insert negotiated terms**] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

k. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

l. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [**insert negotiated terms**], information collected in accordance with Section [**insert section number in contract where provision (i) appears**] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

Permitted Uses and Disclosures by Business Associate

General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

a. Specify purposes:
Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity: [**List Purposes.**]

b. Refer to underlying services agreement:
Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [**insert name of services agreement**], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

a. Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

b. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

d. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

Obligations of the Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose PHI for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate.]

Term and Termination

a. Term. The Term of this Agreement shall be effective as of [insert effective date] and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]

b. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

    1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

    2. Immediately terminate this Agreement [and the _____ Agreement/sections ____ of the _____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or

    3. If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary. [Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

c. Effect of Termination.

    1. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

    2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [insert negotiated terms] that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and

disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

Miscellaneous

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

c. Survival. The respective rights and obligations of Business Associate under Section [insert section number related to "effect of termination"] of this Agreement shall survive the termination of this Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

C. 42 CFR Part 2 Qualified Service Organizations (QSOs)

A qualified service organization (42 CFR § 2.11) means an individual or entity which:

- Provides services to a [42 CFR Part 2 defined] "program," such as data processing; bill collecting; dosage preparation; laboratory analyses; or legal, **medical**, accounting, **or other professional services**, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy; and

- Has entered into a written agreement [a **qualified service organization agreement** (QSOA)] with a program under which that person:
  - Acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from the programs, it is fully bound by these regulations; and
  - If necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by these regulations.

D. 42 CFR Part 2 Qualified Service Organization Agreements (QSOAs)

42 CFR Part 2 Subpart B § 2.12(c)(4) permits federally assisted programs to sign "**qualified service organization agreements**" (or QSOAs) with QSOs, allowing them to disclose only the patient identifying information that is needed to provide services to the program. In the agreements, the outside providers acknowledge that in receiving, storing, processing, or otherwise dealing with patients' records, they are fully bound by 42 CFR Part 2 and promise to safeguard the information, including resisting in judicial proceedings any effort to obtain access to the information, except as permitted by the 42 CFR Part 2 regulations.

A QSOA under 42 CFR Part 2 is similar but not identical to a business associate agreement (45 CFR §§ 164.314(a) and 164.504(e) of the HIPAA Security and Privacy Rules). A QSOA is a two-way written agreement or mechanism that allows for disclosure of patient identifying information between a 42 CFR Part 2 federally assisted program and a QSO that provides any of the services described in C. above to the program. Once a QSOA is in place, 42 CFR Part 2 permits the program to freely communicate information from patients' records to the QSO **as long as it is limited to that information needed** by the QSO **to provide services to the program**. The QSO may also communicate with the 42 CFR Part 2 program and share information it receives from the program back with the program.

A sample contract that complies with both HIPAA (for medical and mental health information) and 42 CFR Part 2 (for substance abuse information) is provided later within this appendix to use as a starting point to develop a federally compliant contract between the entity/program and a business associate/qualified service organization.

1. Patient Consent and QSOAs

- Patient consent is not required when a 42 CFR Part 2 program has entered into a QSOA with an entity that provides any of the covered services (identified in C. 42 CFR Part 2 Qualified Service Organizations), and where the information exchanged is needed to provide the covered services.

- Patient consent is not required when information is exchanged within a 42 CFR Part 2 program or between a 42 CFR Part 2 program and an entity that has direct administrative control over the program. For example, when a substance use disorder unit is a component of a larger behavioral health program or of a general health program, specific information about a patient arising out of that patient's diagnosis, treatment, or referral to treatment can be exchanged without patient consent among the 42 CFR Part 2 program personnel and with administrative personnel who, in connection with their duties, need to know information (42 CFR § 2.12(c)(3)). Patient information **may not be exchanged**, however, among all of the programs and personnel that fall under the umbrella of the entity that has administrative control over the 42 CFR Part 2 program. A QSOA would be required to enable information exchange without patient consent in this situation.

E. Sample QSOA/BAA

HIPAA-covered entities and 42 CFR Part 2 federally assisted programs must meet federal requirements if they are going to form contractual relationships (QSOAs/BAAs) with outside organizations. If an outside organization does not meet the definition of a business associate or qualified service organization and if the individual's status does not fall within HIPAA's lawful custody exception (only for medical and mental health information), then signed, documented, and implemented consent authorizations will be required in order to disclose PHI.

A sample contract that complies with both HIPAA (for medical and mental health information) and 42 CFR Part 2 (for substance abuse information) is provided next in this appendix to use as a starting point to develop a federally compliant contract between the entity/program and a business associate/qualified service organization.[44]

[44] Sample Qualified Service Organization/Business Associate Agreement, Legal Action Center, www.lac.org/doc_library/lac/publications/QSO-BA%20Agreement%20Form.pdf.

Sample Qualified Service Organization Agreement/Business Associate Agreement

The **[insert name of the covered entity and/or federally assisted program providing PHI]** (the "Entity/Program") and the **[insert name of the business associate receiving PHI from the entity/program]** (the "Business Associate") hereby enter into an Agreement whereby the Entity/Program agrees to provide

_____

(Nature of services to be provided to the Center)

Definitions

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Privacy Rule.

a. Business Associate. "Business Associate" shall mean the [**insert name of agency receiving the PHI from the Entity/Program**].

b. Covered Entity/Program. "Covered Entity/Program" shall mean [**insert name of covered entity and/or federally assisted program providing PHI to the Business Associate**].

c. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

d. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

e. Protected Health Information. For the purposes of this Agreement, "Protected Health Information" or "PHI" shall refer to medical and mental health information (45 CFR § 160.103), as well as to substance abuse testing and treatment information, and is limited to the information created or received by the Business Associate from or on behalf of Covered Entity.

f. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

g. Secretary. "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or designee.

Obligations and Activities of Business Associate

Further, the [**name of Business Associate**]:

1. Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received from the Entity/Program identifying or otherwise relating to patients of the Entity/Program ("protected health information" or "PHI"), it is fully bound by the provisions of the federal regulations governing the Confidentiality of Substance Abuse Patient Records, 42 CFR Part 2; and the Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Parts 142, 160, 162 and 164, and may not use or disclose the information except as permitted or required by this Agreement or by law.

2. Agrees to resist any efforts in judicial proceedings to obtain access to the PHI except as expressly provided for in the regulations governing the Confidentiality of Substance Abuse Patient Records, 42 CFR Part 2.

3. Agrees to use appropriate safeguards [**define with more specificity**] in accordance with the HIPAA Security Rule, per the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Subtitle D-Privacy, PART 1—Improved Privacy Provisions and Security Provisions, Section 13401, to prevent the unauthorized use or disclosure of the PHI.

4. Agrees to comply with the security administrative, physical, and technical safeguards requirements in 45 CFR Part 164 Subpart C §§ 164.306, 164.308, 164.310, and 164.312, as well as with the HIPAA Security Rule's policies and procedures and documentation requirements in § 164.316 in the same manner as these requirements apply to covered entities, and agrees that it is civilly and criminally liable for violations of these provisions, per the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Subtitle D-Privacy, PART 1—Improved Privacy Provisions and Security Provisions, Section 13401.

5. Agrees to report to the Entity/Program any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware [**insert negotiated time and manner terms**].

6. Agrees to report breaches of unsecured PHI to the Entity/Program, as required by § 164.410.

7. Agrees to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of PHI by the Business Associate in violation of the requirements of this Agreement.

8. [Agrees to ensure that any agent, including a subcontractor, to whom the Business Associate provides the PHI received from the Entity/Program, or created or received by the Business Associate on behalf of the Entity/Program, agrees to the same restrictions and conditions that apply through this Agreement to the Business Associate with respect to such information.]*****

9. Agrees to provide access to the PHI at the request of the Entity/Program, or to an individual as directed by the Entity/Program, in order to meet the requirements of 45 CFR 164.524, which provides patients with the right to access and copy their own PHI [insert negotiated time and manner terms].

10. Agrees to make any amendments to the PHI as directed or agreed to by the Entity/Program pursuant to 45 CFR § 164.526 [insert negotiated time and manner terms].

11. Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from the Entity/Program, or created or received by the Business Associate on behalf of the Entity/Program, to the entity or to the Secretary of the U.S. Department of Health and Human Services (HHS) for purposes of the Secretary determining the Entity's/Program's compliance with HIPAA [**insert negotiated time and manner terms**].

12. [Agrees to document disclosures of PHI, and information related to such disclosures, as would be required for the Entity/Program to respond to a request by an individual for an accounting of disclosures in accordance with 45 CFR § 164.528 [**insert negotiated time and manner terms**].]*****

13. Agrees to provide the Entity/Program or an individual information in accordance with paragraph (11) of this Agreement to permit the Entity/Program to respond to a request by an individual for an accounting of disclosures in accordance with 45 CFR § 164.528 [insert negotiated time and manner terms].

Permitted Uses and Disclosures by the Business Associate

General Use and Disclosure Provisions **[(a) and (b) are alternative approaches]**

a. Specify purposes:

Except as otherwise limited in this Agreement, the Business Associate may use or disclose PHI on behalf of, or to provide services to, the Entity/Program for the following purposes, if such use or disclosure of PHI would not violate the Privacy Rule if done by Entity/Program or the minimum necessary policies and procedures of the Entity/Program: [**List Purposes.**]

[Optional sample purposes. Customize a list of purposes for the use and disclosure of PHI.]

1) To increase the effectiveness and efficiency of the intake and classification process by providing access to medical, mental health, and substance abuse testing and treatment information.

2) Produce a more accurate and complete profile of sentenced offenders.

3) Reduce recidivism by helping to ensure that offenders—whether in a community or an incarceration setting—receive education, vocational, rehabilitation, and/or treatment services matched to their individual needs.

4) Improve continuity of services provided to offenders as they move from incarceration to community supervision.

b. Refer to underlying services Agreement: **[Optional—only use if an applicable services agreement exists.]** Except as otherwise limited in this Agreement, the Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, the Entity/Program as specified in [**insert name of services**

agreement], provided that such use or disclosure would not violate the Privacy Rule if done by the Entity/Program or the minimum necessary policies and procedures of the Entity/Program.

Specific Use and Disclosure Provisions **[only necessary if parties wish to allow the Business Associate to engage in such activities**]

a. Except as otherwise limited in this Agreement, the Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

b. Except as otherwise limited in this Agreement, the Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Except as otherwise limited in this Agreement, the Business Associate may use PHI to provide Data Aggregation services to the Entity/Program as permitted by 45 CFR § 164.504(e)(2)(i)(B).

d. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

Obligations of the Entity/Program

Provisions for Entity/Program to Inform Business Associate of Privacy Practices and Restrictions **[provisions dependent on business arrangement]**

a. The Entity/Program shall notify the Business Associate of any limitation(s) in its notice of privacy practices of the Entity/Program in accordance with 45 CFR § 164.520, to the extent that such limitation may affect the Business Associate's use or disclosure of PHI.

b. The Entity/Program shall notify the Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

c. The Entity/Program shall notify the Business Associate of any restriction to the use or disclosure of PHI that the Entity/Program has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

Permissible Requests by the Entity/Program

The Entity/Program shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Entity/Program. [Include an exception if the Business Associate will use or disclose PHI for, and the contract includes provisions for, data aggregation or management and administrative activities of the Business Associate.]

Term and Termination

a. Term. The Term of this Agreement shall be effective as of [**insert effective date**], and shall terminate when all of the PHI provided by the Entity/Program to the Business Associate, or created or received by the Business Associate on behalf of the Entity/Program, is destroyed or returned to the Entity/Program, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section. [**Insert negotiated time and manner terms**]

b. Termination for Cause. Upon the Entity's/Program's knowledge of a material breach by the Business Associate, the Entity/Program shall either:

1. Provide an opportunity for the Business Associate to cure the breach or end the violation and terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if the Business Associate does not cure the breach or end the violation within the time specified by the Entity/Program;

2. Immediately terminate this Agreement [and the _____ Agreement/sections ____ of the _____ Agreement] if the Business Associate has breached a material term of this Agreement and cure is not possible; or

3. If neither termination nor cure are feasible, the Entity/Program shall report the violation to the Secretary, HHS. [Bracketed language in this provision may be necessary if there is an underlying services Agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

c. Effect of Termination.

1. *Except as provided in paragraph (2) of this section (c.), upon termination of this Agreement, for any reason, the Business Associate shall return or destroy all PHI received from the Entity/Program, or created or received by the Business Associate on behalf of the Entity/Program. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of the PHI.

2. In the event that the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide to the Entity/Program notification of the conditions that make return or destruction infeasible. Upon **[insert negotiated terms]** that return or destruction of PHI is infeasible, the Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such PHI.

Miscellaneous

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the Entity/Program to comply with the requirements of the HIPAA Privacy and Security Rules, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and 42 CFR Part 2.

c. Survival. The respective rights and obligations of the Business Associate under **Section [insert section number related to "effect of termination"]** of this Agreement shall survive the termination of this Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit the Entity/Program to comply with the HIPAA Security and Privacy Rules.

IN WITNESS WHEREOF, the persons signing below certify that they are duly authorized to sign for, and on behalf of, their respective Party and do hereby execute this contract.

Executed this ____ day of _____, _____.

_____	_____
[Title]	[Title]
[Name of the Business Associate]	[Name of Entity/Program]
[Address]	[Address]

*****Although HIPAA requires these paragraphs to be included in Business Associate Agreements, 42 CFR § 2.11 requires qualified service organizations to abide by the federal drug and alcohol regulations which prohibit such organizations from redisclosing any patient identifying information even to an agent or subcontractor. Legal Action Center has asked HHS for an opinion on this issue.

Appendix E—Court Orders

A. HIPAA and Court Orders[45]

A HIPAA-covered entity may disclose PHI without consent authorization in response to an order of a court or administrative tribunal, provided that the covered entity discloses only the PHI expressly authorized by the order. In the absence of a court order, a covered entity may disclose PHI in response to a subpoena, discovery request, or other lawful process if the covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to give notice of the request to the individual who is the subject of the PHI or that reasonable efforts have been made to attain a qualified protective order for the PHI. The specific HIPAA regulations regarding court orders are listed below.

Per 45 CFR § 164.512:

(e)(1), A covered entity may disclose PHI in the course of any judicial or administrative proceeding:

(i.) In response to an order of a court or administrative tribunal, provided that the entity discloses only the PHI expressly authorized by the order; or

(ii.) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A.) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request; or

(B.) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii.) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking PHI if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A.) The party requesting PHI has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B.) The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C.) The time for the individual to raise objections to the court or administrative tribunal has elapsed and:

[45] www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/courtorders.html.

(1.) No objections were filed; or
(2.) All objections filed by the individual have been resolved by the court or administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv.) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking PHI, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A.) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B.) The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

(v.) For the purposes of paragraph (e)(1) of this section, a qualified protective order means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A.) Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and

(B.) Requires the return to the covered entity or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

(vi.) Notwithstanding (e)(1)(ii) of this section, a covered entity may disclose PHI in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.

B. 42 CFR Part 2 and Court Orders

Note: The sample court order contained in this appendix <u>does not</u> meet the very limited exception of 42 CFR Part 2.

1. **Disclosure of Confidential Communications**

In accordance with 42 CFR Part 2 Subpart E § 2.63, [regarding disclosure of substance abuse information], a court order **may authorize disclosure** of confidential communications made by a patient to a program in the course of diagnosis, treatment, or referral for treatment [of substance abuse] only if:

- The disclosure is necessary to protect against an existing threat to life or of serious bodily injury, including circumstances which constitute suspected child abuse and neglect and verbal threats against third parties;

- The disclosure is necessary in connection with investigation or prosecution of an extremely serious crime, such as one which directly threatens loss of life or serious bodily injury, including homicide, rape, kidnapping, armed robbery, assault with a deadly weapon, or child abuse and neglect; or

- The disclosure is in connection with litigation or an administrative proceeding in which the patient offers testimony or other evidence pertaining to the content of the confidential communications.

2. **Disclosure Not Compelled Without Subpoena or Legal Mandate**

In accordance with 42 CFR Part 2 Subpart E § 2.61, [a court order can be made only] to authorize a disclosure or use of patient identifying information [substance abuse information] which would otherwise be prohibited by 42 U.S.C. 290ee-3, 42 U.S.C. 290dd-3 and these regulations [42 CFR Part 2]. **Such an order does not compel disclosure.** A subpoena or a similar legal mandate must be issued in order to compel disclosure. This mandate may be entered at the same time as and accompany an authorizing court order entered under these regulations.

C. Sample Standing Court Order

The following is a sample standing court order[46] adapted from one drafted by the New York State Office of Court Administration, which allows a program covered by both 42 CFR and HIPAA to use the irrevocable criminal justice consent form permitted under 42 CFR § 2.35 for all patients of that particular program. Note: State laws and court rules may affect the content of court or administrative orders, as well as the proper procedure for seeking and issuing such an order. Not all jurisdictions recognize these court orders. Entities are encouraged to check with their state and local court rules to determine whether a standing court order is authorized in their areas and always to consult with local counsel on matters of state law.

[46] Order to Disclose Protected Health Information, Legal Action Center, www.lac.org/doc_library/lac/publications/sample%20standing%20court%20order.pdf.

Order to Disclose Protected Health Information

The court having reviewed all evidence, progress reports, and relevant regulations and procedures, hereby finds:

1. The above-referenced [individual, offender] is currently an inmate at the [name of correctional entity] serving time for criminal offense(s).

2. The [individual, offender] has been authorized by [name of parole board or authorizing authority] to be released from [name of correctional entity] under supervised [probation, parole] for the following period of time [insert period of time].

3. The court requires timely and accurate information concerning the [individual's, offender's] attendance and progress in treatment in order to adequately monitor the effectiveness and progress of the [individual's, offender's] continued participation in [probation, parole].

4. The [individual, offender] has been released from [name of correctional entity] in accordance with the following court-ordered conditions:

    a. The [individual, offender] will report [insert time period] to a court-appointed [probation, parole] officer; and

    b. The [individual, offender] will participate in a [substance abuse treatment, behavioral health, or other health-care] program provided by [insert name of treatment or health-care provider(s)]; and

    c. The [name of treatment or health care provider(s)] will disclose the [individual's, offender's] progress in the treatment program to the court by way of routine status reports provided to the court-appointed [probation, parole] officer, and

    d. The reported treatment progress will include, as applicable, treatment recommendations, diagnosis, attendance, scope of treatment, treatment progress and quality of participation, dates and results of toxicology testing, and termination or completion of treatment concerning the above-named [individual, offender].

5. The privacy regulations promulgated by the United States Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 CFR Parts 160 and 164, have imposed restrictions on the ability of health-care providers to disclose protected health information (PHI) concerning a particular individual to third parties except under particular circumstances; and

6. HIPAA's privacy regulations contain an exception permitting health-care providers to disclose PHI "in the course of any judicial or administrative proceeding . . . in response to an order of a court or administrative tribunal" (45 CFR § 164.512(e)(1)).

THEREFORE, IT IS HEREBY ORDERED:

Pursuant to HIPAA, [insert name of treatment or health-care provider] shall disclose to the [individual's, offender's] court-appointed [probation, parole] officer and/or the staff of this court, subject to the federal regulations governing the Confidentiality of Substance Abuse Patient Records (42 CFR Part 2), information concerning, as applicable, the treatment recommendations, diagnosis, attendance, scope of treatment, treatment progress and quality of participation, dates and results of toxicology testing, and termination or completion of treatment concerning the above-named [individual, offender]. Any application for disclosure of information pursuant to 42 CFR Part 2 shall be made in accordance with 42 CFR §§ 2.61–2.65 and other applicable sections.

DATED: _____ Judge/Justice_____

Appendix F—42 CFR 2.22: Notice to Patients of Federal Confidentiality Requirements

Federally assisted programs (refer to definition in Appendix A), in accordance with 42 CFR Part 2 Subpart B § 2.22, for individuals tested, diagnosed, and/or treated for substance abuse, at the time of admission or as soon thereafter as the patient is capable of rational communication, shall communicate to the patient that federal law and regulations protect the confidentiality of alcohol and drug abuse patient records; and give to the patient a summary in writing of the federal law and regulations.

To comply with this requirement, the written summary of the federal law and regulations must include:

1. A general description of the limited circumstances under which a program may acknowledge that an individual is present at a facility or disclose outside the program information identifying a patient as an alcohol or drug abuser.

2. A statement that violation of the federal law and regulations by a program is a crime and that suspected violations may be reported to appropriate authorities in accordance with these regulations.

3. A statement that information related to a patient's commission of a crime on the premises of the program or against personnel of the program is not protected.

4. A statement that reports of suspected child abuse and neglect made under state law to appropriate state or local authorities are not protected.

5. A citation to the federal law and regulations.

Ways to Use This Notice

1. The entity may devise its own notice or may use the **sample notice** shown below to comply with the requirement to provide the patient with a summary in writing of the federal law and regulations.

2. **For situations where an individual has been released on probation or parole and the entity must provide notice of its privacy practices, this notice may be combined with the HIPAA Notice of Privacy Practices (refer to Appendix F for a sample of HIPAA notice).**

3. Further, the program may include information concerning any applicable state law and any program policy that is **not inconsistent** with state and federal law on the subject of confidentiality of alcohol and drug abuse patient records.

Note: A similar notice is included on the last page of the sample consent authorization form contained in Appendix C.

Sample Notice—Confidentiality of Alcohol and Drug Abuse Patient Records

The confidentiality of alcohol and drug abuse patient records maintained by [name of entity] is protected by federal law and regulations. Generally, the [name of entity] may not say to a person outside the program that a patient attends the program, or disclose any information identifying a patient as an alcohol or drug abuser unless: 1.) the patient consents in writing; 2.) the disclosure is allowed by a court order; or 3.) the disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation purposes.

Violation of the federal laws and regulations by a program is a crime. Suspected violations may be reported to appropriate authorities in accordance with federal regulations. Federal laws and regulations do not protect any information about a crime committed by a patient either at the program or against any person who works for the program or about any threat to commit such a crime. Federal laws and regulations do not protect any information about suspected child abuse or neglect from being reported under state law to appropriate state or local authorities. (See 42 U.S.C. 290dd-3 and 42 U.S.C. 290ee-3 for federal laws and 42 CFR Part 2 for federal regulations.)

Appendix G—PHI Privacy Policy Review Checklist

The purpose of this PHI Privacy Policy Review Checklist is to provide privacy policy authors, project teams, and agency administrators with a useful tool for evaluating whether the provisions contained within their entity's PHI policies have adequately satisfied the core requirements of HIPAA (for medical and mental health information) and, if applicable, 42 CFR Part 2 (for substance abuse information).

The checklist is a useful way to assess existing PHI policies—whether contained in one document or whether PHI provisions are scattered across multiple departmental or agency policies, as well as a tool to use during the drafting process to check work on the draft policy, during the final review of the policy, or to utilize to perform an annual PHI policy. It will reveal gaps or areas where minor enhancement or additional provisions are needed to ensure that PHI policies addressing all of the recommended core policy concepts:

A. Purpose statement
B. Policy applicability and legal compliance
C. Governance and oversight
D. Definitions
E. Information
F. Acquiring and receiving information
G. Information quality assurance
H. Program evaluation and research
I. Merging records
J. Use and disclosure
K. Redress
    K.1 Disclosure
    K.2 Data amendments
    K.3 Appeals
L. Information security safeguards
M. Information retention and destruction
N. Accountability and enforcement
    N.1 Information system transparency
    N.2 Accountability
    N.3 Enforcement
O. Training

A. How to Use This Checklist

The format of this checklist was designed to exactly mirror the structure and provisions contained in Chapter 3. PHI Policy Development Template. With both the agency PHI privacy policy(ies) and this checklist in hand, reviewers are guided to read each question in the checklist; compare it with the language in the PHI policy (noting the policy name or number where provision is addressed, and the section and page number for later reference and revision purposes);

and indicate whether the provision has been fully met, partially met, was not addressed, or if the recommended provision is not applicable. Comments and suggestions can be added where needed for follow-up and policy refinement.

For those entities that developed their PHI policies using the template in Chapter 3, completing this checklist should be a simple process, since each checklist question sequentially mirrors the structure of the PHI Policy Development Template. Thus the reviewer will find it a fluid process to move through both documents in tandem as the review is performed. Policy authors are not required, however, to follow the outline and format of the PHI Policy Development Template in order to use this checklist. The checklist will still readily illuminate for the reviewer whether each recommended provision has been satisfied, requiring only minor additional effort to locate the policy language in the draft or existing policy(ies) in order to score it in the checklist.

B. Annual Review

This checklist is also designed for use in performing the annual PHI policy review. As a general rule, entities are encouraged to review and update the PHI privacy protection provisions, contained in their PHI privacy policy(ies) at least **annually**. Annual updates will ensure that appropriate revisions are made in response to changes in applicable laws, technology, the purpose and use of the information systems, and public expectations. This, in turn, will ensure that systems and individuals are enabled to comply with the most current protections established in the entity PHI privacy policy.

C. Checklist Column Headings

To assist reviewers in navigating the policy review checklist, the following information is provided to describe the purpose and use of each of the checklist's column headings.

Template Section—Each question is grouped according to core policy provision concepts and reflects Sections A. through O. of the PHI Policy Development Template. This column indicates the template section in which the question is contained.

Does the entity's PHI privacy policy clearly state the following?—Each recommended provision in the PHI Policy Development Template is reworded here as an evaluation question, asking the reviewer whether the entity's PHI privacy policy has addressed the relevant template provision. Questions are numbered in the exact same sequence as the provisions in the PHI Policy Development Template.

Cite policy name or number where the provision is covered. Identify section and page number—For cross-referencing and future review purposes (for example, if there is more than one draft), this column enables the reviewer to indicate which entity policy the provision is located in and the section and page number. This is especially useful when a provision, upon review, is found to be partially met; the author can quickly locate the provision in the applicable policy to make the needed revisions.

Criteria met—A checkbox for the reviewer to indicate whether the privacy policy provision has fully satisfied the recommended core concept.

Criteria partially met—A checkbox for the reviewer to indicate that the privacy policy provision only "partially" satisfies the recommended core concept and requires further revision. An explanation should be recorded in the Comments/Suggestions area.

Not applicable (N/A)—A column to indicate that the provision is not applicable to the entity or the entity's functions and procedures. If appropriate, an explanation can be recorded in the Comments/ Suggestions area.

Comments/Suggestions—An area for documenting guidance, suggested language, and other comments (for example, partially met criteria, criteria that were not addressed, or criteria that are not applicable).

Annual Review: Check if provision requires update—A checkbox to be used by the individual performing the annual review to indicate that the provision requires revisions.

Annual Review: Was the provision revised?—A checkbox to be used by the individual performing the annual review to document that the provision was updated.

Annual Review Recommendations—An area for documenting justifications for needed revisions (e.g., legislative change), comments, and other recommendations.

PHI Privacy Policy Review Checklist

Entity Name: _____ **Review Date:** _____

Person Completing Review: _____ **Phone:** _____

Title: _____ **E-mail:** _____

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	**Cite policy name or number where provision is covered. Identify section and page number**	**Check if criteria are met**	**Check if criteria are only partially met**	**Check if provision is not applicable (N/A)**	**Comments/Suggestions**	**Check if provision requires update**	**Was the provision revised?**	**Annual Review Recommendations**
A. Purpose Statement	**1.** The purpose of establishing a privacy, civil rights, and civil liberties protection policy (i.e., what does the entity hope to accomplish in adopting this policy)?		☐	☐			☐	☐ Yes ☐ No	
B. Policy Applicability and Legal Compliance	**1.** Who is subject to the privacy policy (who must comply with the policy; for example, entity personnel, participating agencies, and private contractors)?		☐	☐			☐	☐ Yes ☐ No	
	2. The method(s) by which the policy is made available to personnel, participating entities, and individual users (for example, in print, online, etc.)? Whether the entity requires personnel, participating entities, and individual users to acknowledge receipt of the policy and agreement to comply with the policy in writing?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
	3. That personnel and participating information-originating and user agencies must be in compliance with all applicable law protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of medical, mental health, and substance abuse information? The primary laws with which personnel and participating users must comply?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
	4. Whether the entity's internal operating policies are in compliance with all applicable law protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination of medical, mental health, and substance abuse information? Are the laws with which internal operation policies must be in compliance cited in the privacy policy?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
C. Governance and Oversight	**1.** Who has primary responsibility for the entity's overall operation, including the entity's information systems, information collection and retention procedures, coordination of personnel, and enforcement of the privacy policy? Which individual will ultimately be held accountable for the operation of the information system and for any problems or errors?		☐	☐			☐	☐ Yes ☐ No	
	2. Whether the entity has a privacy oversight committee, team, or individual that is responsible for the development of the PHI privacy policy and/or that will routinely review and update the policy?		☐	☐			☐	☐ Yes ☐ No	
	3. Whether there is a designated and trained privacy officer (or privacy officer function) within the entity who will handle reported errors and violations and oversee the implementation of PHI privacy protections? Does the policy identify the title of the individual who will serve as the privacy officer, whether a full-time privacy officer position or the occupant of a different position, such as the assistant director or entity counsel? The contact information for the privacy officer (for example, phone, Web site, e-mail, or U.S. mail address)?		☐ ☐ ☐	☐ ☐ ☐			☐ ☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No	
	4. Who is responsible for ensuring that enforcement procedures and sanctions for noncompliance with the PHI privacy policy are adequate and enforced?		☐	☐			☐	☐ Yes ☐ No	
D. Definitions	**1.** The key words or phrases (and definitions) that are regularly used in the policy for which the entity wants to specify particular meanings?		☐	☐			☐	☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	**Cite policy name or number where provision is covered.** **Identify section and page number**	**Check if criteria are met**	**Check if criteria are only partially met**	**Check if provision is not applicable (N/A)**	**Comments/Suggestions**	**Check if provision requires update**	**Was the provision revised?**	**Annual Review Recommendations**
E. Information	**1.** What information may be sought, retained, shared, disclosed or disseminated, by the entity? Whether there are different policy provisions for different types of information (e.g., medical, mental health, and substance abuse information, as well as fact-based information databases)?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
	2. The purpose(s) for which information **may be** sought, retained, shared, disclosed, or disseminated by the entity?		☐	☐			☐	☐ Yes ☐ No	
	3. What information **may not** be sought, retained, shared, disclosed, or redisclosed by the entity (e.g., for reasons of discrimination)?		☐	☐			☐	☐ Yes ☐ No	
	4. Whether the entity applies labels (by record, data set, or system of records) to the maximum extent feasible, to entity-originated PHI (or ensures that the PHI-providing entity has applied labels) to indicate to the accessing authorized information recipient that: o The information is "protected health information," including personally identifiable information on any individual regardless of citizenship or U.S. residency status? o The information has applicable limitations on access and sensitivity of disclosure, is subject to specific health information privacy or other similar restrictions and, if so, the nature of such restrictions? o The laws that restrict who can access information, how information can be used, and the retention or disclosure of certain types of information?		☐ ☐ ☐	☐ ☐ ☐			☐ ☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No	
	5. Whether the entity categorizes information (or ensures that the PHI-providing entity has categorized information) based on its nature (for example, conditions of supervision, medical, mental health, and substance abuse information), usability, and quality?		☐	☐			☐	☐ Yes ☐ No	
	6. The conditions that prompt the labels cited in E.4 and E.5 to be reevaluated?		☐	☐			☐	☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
	7. Whether the entity requires certain basic descriptive information (metadata tags or labels) to be entered and associated with each record, data set, or system of records containing PHI that will be accessed, used, and disclosed? • Basic information may include, where relevant and appropriate: the name of the PHI-providing entity, department, component, or subcomponent (if applicable). • If applicable, the name of the entity's information system from which the information is disseminated. • The date the information was collected (submitted) and, where feasible, the date its accuracy was last verified. • The title and contact information for the person to whom questions regarding the information, including its accuracy, should be directed.		☐	☐			☐	☐ Yes ☐ No	
	8. Whether the entity maintains a record of the source of the information sought and collected?		☐	☐			☐	☐ Yes ☐ No	
F. Acquiring and Receiving Information	**1.** Whether the agencies that access your entity's PHI and/or share PHI with your entity ensure that they will adhere to applicable laws and policies?		☐	☐			☐	☐ Yes ☐ No	
	2. Whether the entity contracts with commercial databases and, if so, how the entity ensures that the commercial database company is in legal compliance in its information-gathering techniques?		☐	☐			☐	☐ Yes ☐ No	
G. Information Quality Assurance	**1.** Whether the entity has established procedures and procedures (manual and electronic) to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the PHI it collects, maintains, and disseminates?		☐	☐			☐	☐ Yes ☐ No	
	2. Whether the entity researches alleged or suspected errors and deficiencies (or refers them to the PHI-providing agency)? How the entity responds to confirmed errors or deficiencies?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
	3. When the entity reviews the quality of the **PHI it <u>originates</u>** and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, the entity's procedure for correction or destruction?		☐	☐			☐	☐ Yes ☐ No	
	4. When the entity reviews the quality of the **PHI it has <u>received from</u> an originating agency** and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, whether the entity notifies the originating agency or the originating agency's privacy officer? The method used to notify the agency (written, telephone, or electronic notification)?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
	5. When the entity reviews the quality of the **PHI it has <u>provided to</u> an external agency** and identifies data that may be inaccurate or incomplete, includes incorrectly merged information, is out of date, cannot be verified, has a questionable source, or lacks adequate context such that the rights of the individual may be affected, whether the entity notifies the external agency? The method used to notify the agency (written, telephone, or electronic notification)?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
	6. If the entity is a HIPAA-covered entity, the entity's procedure for amending PHI if informed by another covered entity of a need to amend an individual's record?		☐	☐			☐	☐ Yes ☐ No	
H. Collation and Analysis	**1.** Who is authorized (position/title, credentials, etc.) to analyze deidentified PHI for evaluation and research purposes?		☐	☐			☐	☐ Yes ☐ No	
	2. What information is analyzed?		☐	☐			☐	☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
	3. For what purpose(s) is the deidentified PHI analyzed?		☐	☐			☐	☐ Yes ☐ No	
I. Merging Records	**1.** Who is authorized (position/title, credentials, etc.) to merge records?		☐	☐			☐	☐ Yes ☐ No	
	2. What matching criteria the entity requires when attempting to merge PHI from multiple records allegedly about the same individual? In other words, when two records are compared for possible merger, are there certain attributes (name, date of birth, social security number, etc.) that must match, or is there a minimum number of attributes (for example, two out of five) that must match to link the two records as relating to the same person?		☐	☐			☐	☐ Yes ☐ No	
	3. If the criteria specified in I.2 are not met, the entity's procedure for associating records? **Note:** If the entity does not merge or associate records that have partial matches, then the policy should so state.		☐	☐			☐	☐ Yes ☐ No	
J. Sharing and Disclosure	**1.** What types of information recipient actions and permissions are controlled by the entity's access or dissemination limitations? Best practice: It is suggested that entities specify their method for identifying information recipient actions and permissions in their privacy policies. **Note:** Information recipient actions and permissions are often used to identify entities and individuals with a need and right to know particular information; to access case management information (including medical, mental health, and/or substance abuse information); access nonpersonally identifiable information only; or to identify who is authorized to submit or modify particular records or record sets, to have read-only access or to be authorized to add/modify/delete records, or to be authorized to grant privileges.		☐	☐			☐	☐ Yes ☐ No	
	2. What limitations the entity has implemented to limit or restrict disclosure of PHI?		☐	☐			☐	☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
	3. The conditions and credentials by which access to and disclosure of PHI records retained by the entity will be provided **within the entity or in other governmental agencies**? Whether an audit trail is kept of access to and disclosure of PHI retained by the entity (e.g., dissemination logs, algorithms)?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
	4. The conditions by which access to and disclosure of PHI retained by the entity are **not permitted without an individual consent authorization**?		☐	☐			☐	☐ Yes ☐ No	
	5. Whether the entity permits released individuals (those who are no longer in lawful custody) to request that the entity restrict the use and disclosure of the individuals' PHI retained by the entity?		☐	☐			☐	☐ Yes ☐ No	
	6. For individuals who are released from custody (for example, on probation or parole), the conditions by which the entity may use or disclose PHI without the individuals' written consent authorization?		☐	☐			☐	☐ Yes ☐ No	
	7. Whether participating agencies that access information from the entity are required to obtain approval from the originator of the information prior to further dissemination or to follow the disclosure or redisclosure law applicable to the originating agency? If the information is substance abuse information, does the entity provide the required 42 CFR Part 2 notice covering the disclosure of such information, along with any such disclosure of the substance abuse information?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
	8. The conditions under which access to and disclosure of PHI records retained by the entity will be provided **to those responsible for medical, mental health and/or behavioral health, including substance use services**? Whether an audit trail is kept of access to and disclosure of information retained by the entity (e.g., dissemination logs, algorithms)?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
	9. Under what circumstances and what legal authority will access to and disclosure of a record be provided **to a member of the public** in response to an information request, and whether these circumstances are described in the entity's redress policy?		☐	☐			☐	☐ Yes ☐ No	
	Whether an audit trail is kept of access to and disclosure of information retained by the entity without the audit trail constituting an impermissible collection of information of a member of the public (e.g., dissemination logs, algorithms)? **Note:** This does not apply to circumstances in which an entity chooses to provide nonsensitive information to the public or to provide sensitive information in accordance with entity policy in response to an emergency situation.		☐	☐			☐	☐ Yes ☐ No	
	10. The conditions under which release of information retained by the entity can be made **for specific purposes or to specific persons**?		☐	☐			☐	☐ Yes ☐ No	
	Whether an audit trail is kept showing how those conditions were met?		☐	☐			☐	☐ Yes ☐ No	
	11. Under what circumstances and to whom the entity will **not disclose** PHI records?		☐	☐			☐	☐ Yes ☐ No	
	12. The categories of records that ordinarily will **not be provided to the public** pursuant to applicable legal authority?		☐	☐			☐	☐ Yes ☐ No	
	Citations to applicable legal authority for each stated category?		☐	☐			☐	☐ Yes ☐ No	
	13. The entity's policy on confirming the existence or nonexistence of information to persons or agencies that are not eligible to receive the information?		☐	☐			☐	☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
K. Redress **K.1 Disclosure**	**Disclosure** **1.** If required by state statute or federal law, the conditions under which the entity will disclose PHI contained in the entity's designated record set to an individual about whom the information was gathered? Whether a record is kept of all requests and of what information is disclosed to an individual? **Note:** If the state public (open) records act provides procedures for disclosure, corrections, appeals, and handling of complaints when information is not subject to disclosure, these procedures should be summarized in the privacy policy in lieu of using the sample language provided in the privacy template for that type of information.		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
	2. If the entity is a HIPAA-covered entity, the conditions under which the covered entity will transmit a copy of an individual's PHI from the entity's designated record set to a third-party person if requested and designated by the individual?		☐	☐			☐	☐ Yes ☐ No	
	3. The conditions under which the entity **will not disclose information to an individual** about whom information has been gathered? Citations to applicable legal authority for each stated basis (condition) for denial? Whether the entity refers the individual to the agency originating the information?		☐ ☐ ☐	☐ ☐ ☐			☐ ☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No	
K.2 Data Amendments	**Data Amendments** **1.** If the entity is a HIPAA-covered entity, the point of contact for handling individuals' requests for amendments of PHI in the designated record set? Whether the entity retains documentation of the titles of the person(s) or office(s) responsible?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
K.3 Appeals	**2.** The entity's procedure for handling individuals' requests for correction (or amendments) involving **information in a designated record set that the entity can change because it originated the information**? Whether the entity maintains a record of requests for corrections (amendments)?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
	Appeals **1.** The conditions under which the entity may deny an individual's request for **access** or **correction (amendment)**?		☐	☐			☐	☐ Yes ☐ No	
	2. If requests for access or corrections (amendments) are denied, the entity's procedure for appeal (or review)?		☐	☐			☐	☐ Yes ☐ No	
L. Information Security Safeguards	**1.** Whether the entity has a designated information security officer? Whether training is provided for the information security officer? If the role is a component of another position, whether the policy identifies the title of the position upholding security officer responsibilities?		☐ ☐ ☐	☐ ☐ ☐			☐ ☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No	
	2. The entity's physical, procedural, and technical safeguards for ensuring the security of entity data? (Does the policy describe how the entity will protect the information from unauthorized access, modification, theft, sabotage, or destruction [whether internal or external] resulting from natural or human-caused disasters or intrusions with, for example, procedures, practices, system protocols, use of software, information technology tools, process for data backups, and physical security measures?)		☐	☐			☐	☐ Yes ☐ No	
	3. The requirements that ensure that the information will be stored in a secure format and a secure environment?		☐	☐			☐	☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
	4. If the entity is a HIPAA-covered entity, whether the entity has conducted an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the entity?		☐	☐			☐	☐ Yes ☐ No	
	5. The required credentials of entity personnel authorized to have access to entity information?		☐	☐			☐	☐ Yes ☐ No	
	6. Whether electronic access to entity data identifies the user?		☐	☐			☐	☐ Yes ☐ No	
	7. Whether a log is kept of accessed and disseminated entity data, and whether an audit trail is maintained?		☐	☐			☐	☐ Yes ☐ No	
	8. Whether the entity has electronic procedures for terminating an electronic session after a period of inactivity?		☐	☐			☐	☐ Yes ☐ No	
	9. Whether risk and vulnerability assessments (if maintained) are stored separately from publicly available data?		☐	☐			☐	☐ Yes ☐ No	
	10. The entity's procedures for responding to suspected or known security incidents?		☐	☐			☐	☐ Yes ☐ No	
	11. The entity's procedures for adhering to data breach notification laws or policies?		☐	☐			☐	☐ Yes ☐ No	
M. Information Retention and Destruction	**1.** The entity's review schedule for validating or purging information? The periodic basis for this and/or reference to the applicable law(s)?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
	2. Whether the entity has a retention and destruction policy? What methods the entity employs to remove or destroy PHI? Whether law or policy is referenced, if applicable? **Note:** A retention and destruction policy should be provided for all PHI databases/records held by the entity.		☐ ☐ ☐	☐ ☐ ☐			☐ ☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
	3. Whether a record is kept of dates when information is to be removed (purged) if not validated prior to the end of its period? Whether notification is given prior to removal (for example, an autogenerated system prompt to entity personnel that a record is due for review and validation or purge)?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	
	4. Whether a confirmation of the deletion is kept, including a log of the deletion (e.g., date of deletion).		☐	☐			☐	☐ Yes ☐ No	
N. Accountability and Enforcement **N.1 Information System Transparency**	**Information System Transparency** **1.** Whether the entity's privacy policy is available to the public (for example, provided to the public for review, made available upon request, and/or posted on the entity's Web site—include Web address)?		☐	☐			☐	☐ Yes ☐ No	
	2. If your entity is a HIPAA-covered entity, whether the entity posts its PHI privacy policy on the entity's Web site?		☐	☐			☐	☐ Yes ☐ No	
	3. If your entity is a federally assisted program, whether the entity provides a notice to patients of federal confidentiality requirements (e.g., substance abuse information, 42 CFR Part 2)?		☐	☐			☐	☐ Yes ☐ No	
	4. Whether the entity has a process for individuals to make complaints concerning the entity's policies, procedures, and privacy practices if the individual feels that a violation of HIPAA or 42 CFR Part 2 has occurred?		☐	☐			☐	☐ Yes ☐ No	
	5. Whether the entity has a point of contact (position/title) for handling inquiries or complaints? Whether the contact information for this individual (for example, phone, Web site, e-mail, or U.S. mail address) is provided?		☐ ☐	☐ ☐			☐ ☐	☐ Yes ☐ No ☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	Cite policy name or number where provision is covered. Identify section and page number	Check if criteria are met	Check if criteria are only partially met	Check if provision is not applicable (N/A)	Comments/Suggestions	Check if provision requires update	Was the provision revised?	Annual Review Recommendations
N.2 Accountability	**Accountability**								
	1. Whether access (e.g., electronic or hard-copy access) to the entity's data identifies the user, and whether the identity of the user is retained in the audit log?		☐	☐			☐	☐ Yes ☐ No	
	2. Whether a log (electronic or paper) is kept of accessed and disseminated entity-held data, and whether an audit trail is maintained?		☐	☐			☐	☐ Yes ☐ No	
	3. The procedures and practices the entity follows to enable evaluation of user compliance with information access requirements, the entity's PHI privacy policy, and applicable law?		☐	☐			☐	☐ Yes ☐ No	
	4. Whether the entity has a mechanism for personnel to report errors and suspected or confirmed violations of entity privacy policies related to PHI?		☐	☐			☐	☐ Yes ☐ No	
	5. The entity's retention period for patient consent authorizations, and whether audits are completed to ensure that appropriate consent authorizations are maintained and current?		☐	☐			☐	☐ Yes ☐ No	
	6. Whether audits are completed by an independent third party or a designated representative of the entity?		☐	☐			☐	☐ Yes ☐ No	
	Whether the audits are conducted both annually (or other time period) and randomly?		☐	☐			☐	☐ Yes ☐ No	
	7. How often the entity reviews and updates the provisions contained within the PHI privacy policy (recommendation is annually)?		☐	☐			☐	☐ Yes ☐ No	
	Whether a record is kept of all changes to entity PHI privacy policies, including security provisions and procedures and, if so, the entity's retention period for such documentation?		☐	☐			☐	☐ Yes ☐ No	
N.3 Enforcement	**Enforcement**								
	1. The procedures for enforcement if entity personnel, a participating agency, or an authorized user is suspected of being or has been found to be in noncompliance with the provisions of the entity's PHI privacy policy?		☐	☐			☐	☐ Yes ☐ No	

Template Section	PHI Policy Provision Checklist						Annual Review Checklist		
	Does the entity's PHI privacy policy clearly state the following:	**Cite policy name or number where provision is covered.** **Identify section and page number**	**Check if criteria are met**	**Check if criteria are only partially met**	**Check if provision is not applicable (N/A)**	**Comments/Suggestions**	**Check if provision requires update**	**Was the provision revised?**	**Annual Review Recommendations**
	2. The entity's policy with regard to the qualifications and number of participating agency personnel authorized to access PHI, and the additional sanctions the entity may utilize for violations of the entity's PHI privacy policy?		☐	☐			☐	☐ Yes ☐ No	
O. Training	**1.** What personnel the entity requires to participate in training programs regarding implementation of and adherence to the PHI privacy policy?		☐	☐			☐	☐ Yes ☐ No	
	2. What is covered by the training program (for example, purpose of the policy, substance and intent of the provisions of the policy, security requirements, impact of infractions, and possible penalties for violations)?		☐	☐			☐	☐ Yes ☐ No	

Appendix H—Standards and Resource List

This template incorporates guidelines and requirements contained in many of the following documents, standards, and online resources:

- *A Quick Guide to State Laws on Sensitive Health Information*, Justice and Health Connect, Substance Use and Mental Health Program at the Vera Institute of Justice, supported by the Department of Justice's (DOJ) Bureau of Justice Assistance, www.jhconnect.org/wp-content/uploads/2013/06/State-Health-Laws-fact-sheet-June-23-2013.pdf.

- *Applying the Substance Abuse Confidentiality Regulations 42 CFR Part 2 (Revised)*, SAMHSA, HHS, December 14, 2011, www.samhsa.gov/about/laws/SAMHSA_42CFRPART2FAQII_Revised.pdf.

- *Basics of 42 CFR Part 2*, Justice and Health Connect, Substance Use and Mental Health Program at the Vera Institute of Justice, supported by the Department of Justice's (DOJ) Bureau of Justice Assistance, www.jhconnect.org/wp-content/uploads/2013/06/42-CFR-Part-2-final.pdf.

- Code of Federal Regulations (CFR), Title 28 (28 CFR)—Judicial Administration, Chapter 1—U.S. Department of Justice, Part 23—*Criminal Intelligence Systems Operating Policies*, http://it.ojp.gov/documents/28CFR_Part_23.pdf.

- Confidentiality of Substance Abuse Patient Records, 42 CFR Part 2, Code of Federal Regulations, Title 42: Public Health, Part 2, www.gpo.gov/fdsys/pkg/CFR-2002-title42-vol1/pdf/CFR-2002-title42-vol1-part2.pdf.

- *Corrections, Law Enforcement, and the Courts*, National Governors Association Center for Best Practices, www.nga.org/files/live/sites/NGA/files/pdf/FACTSHIPAACORRECT.pdf.

- *Fair Information Principles*, Organisation for Economic Co-operation and Development (OECD), http://it.ojp.gov/documents/OECD_FIPs.pdf.

- *Frequently Asked Questions—Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)*, Legal Action Center for the SAMHSA, DHHS, www.samhsa.gov/healthprivacy/docs/ehr-faqs.pdf.

- *Frequently Asked Questions About the Disposal of Protected Health Information*, HHS, Office for Civil Rights, www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf.

- *Fundamentals of the Legal Health Record and Designated Record Set*, American Health Information Management Association (AHIMA), www.ahima.org.

- *General Overview of Standards for Privacy of Individually Identifiable Health Information*, 45 CFR Parts 160 and Subparts A and E of Part 164, HHS, OCR, December 3, 2002, Revised April 3, 2003, www.hhs.gov/ocr/privacy/hipaa/understanding/summary/overview.pdf.

- *Guidance for Identifying Designated Record Sets Under HIPAA*, version 2, North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) Designated Record Sets Work Group, Privacy and Confidentiality Focus Group, February 3, 2003, endorsed by the North Carolina Health Information Management Association, www.nchica.org/HIPAAresources/Samples/Guidance.pdf.

- *Guide to Privacy and Security of Health Information*, The Office of the National Coordinator for Health Information Technology, http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

- *Health Information Privacy in the Correctional Environment*, Melissa M. Goldstein, J.D., The George Washington University, issue paper, Community Oriented Correctional Health Services, April 2012, http://www.cochs.org/files/hieconf/PRIVACY.pdf.

- *Health Information Technology . . . What it means for you*, Sandy D. Cogan, SAMHSA Newsletter, Winter 2012, volume 20, number 1, page 3, Substance Abuse and Mental Health Services Administration (SAMHSA), U.S. Department of Health and Human Services (HHS), www.samhsa.gov/samhsanewsletter/Volume_20_Number_1/Winter2012-volume-20-number-1.pdf.

- Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191, www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

- HIPAA, Corrections, Law Enforcement, and the Courts, At-A-Glance, National Governors Association Center for Best Practices, www.nga.org/cms/home/nga-center-for-best-practices/center-publications/page-health-publications/col2-content/main-content-list/title_hipaa-corrections-law-enforcement-and-the-courts.html.

- *HIPAA Privacy in Correctional Healthcare*, Hubbert Systems Consulting, www.hubbertsystems.com/new/dl.cgi/1351039909_19667.f_cis_pdf.pdf/HIPAA%20and%20Correctional%20Health%20Care.pdf.

  This is an FAQ that provides an overview of the applicability of HIPAA in correctional health-care settings. This FAQ explains HIPAA compliance within correctional health settings, including the implications of HIPAA on health information exchanges within correctional health care. It addresses frequently asked questions, including: (1) Are correctional health-care organizations impacted by HIPAA? (2) What health information can correctional health-care organizations use and disclose? (3) What privacy rights do people in correctional facilities have? (4) How does HIPAA apply when a person is released?

- HIPAA Security Rule Toolkit, National Institute of Standards and Technology (NIST), http://scap.nist.gov/hipaa/.

- *HIPAA Survival Guide Omnibus Rule Ready*, fourth edition, Carlos A. Leyva and Mayra L. Scheuermann, http://store.hipaasurvivalguide.com/hipaa-survival-guide-third-edition.html.

- *Information Sharing in Criminal Justice—Mental Health Collaborations: Working with HIPAA and Other Privacy Laws*, John Petrila, J.D., L.L.M, and Hallie Fader-Towe, J.D., Council of State Governments Justice Center, Bureau of Justice Assistance, Office of Justice Programs, DOJ, www.bja.gov/Publications/CSG_CJMH_Info_Sharing.pdf.

- Privacy and Security Toolkit, Healthcare Information and Management Systems (HIMSS), http://www.himss.org/library/healthcare-privacy-security/toolkit?navItemNumber=16480.

- *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* (Privacy Guide), U.S. Department of Justice's (DOJ's) Global Justice Information Sharing Initiative's (Global) Privacy and Information Quality Working Group (GPIQWG), www.it.ojp.gov/privacy.

- *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (SLT Policy Development Template), DOJ's GPIQWG, www.it.ojp.gov/privacy.

- *Privacy Resources Guide*, National Resource Center for Child Welfare Data and Technology (NRC-CWDT), www.nrccwdt.org/wp-content/uploads/2012/03/PrivacyResourceGuide_Apr2012.pdf.

- *Standards for Privacy of Individually Identifiable Health Information*, 45 CFR Parts 160 through 164, HHS, Office of the Secretary, Federal Register, volume 64, no. 212, November 3, 1999, Proposed Rules, www.gpo.gov/fdsys/pkg/FR-1999-11-03/pdf/99-28440.pdf.

- Healthcare, Part VI, *Standards for Treatment of Prisoners*, Standards for Criminal Justice, third edition, American Bar Association, www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/Treatment_of_Prisoners.authcheckdam.pdf.

- *Sequential Intercepts for Developing Criminal Justice (CJ)-Mental Health (MH) Partnerships*, National GAINS Center, http://gainscenter.samhsa.gov/pdfs/integrating/GAINS_Sequential_Intercept.pdf.

  The Sequential Intercept Model (SIM) is a conceptual map of the points in the criminal justice system in which there are opportunities to divert people from incarceration and link them to treatment. Agencies can use SIM to identify their information sharing needs and brainstorm ways to close silos between criminal justice and community health systems.

- *Summary of the HIPAA Privacy Rule*, HHS, OCR, May 2003, www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

- *Summary of the HIPAA Security Rule*, Health Information Privacy, HHS, http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.

- *The Confidentiality of Substance Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Substance Abuse Programs*, HHS, Substance Abuse and Mental Health Services Administration, Center for Substance Abuse Treatment, June 2004, www.samhsa.gov, available at http://store.samhsa.gov/product/The-Confidentiality-of-Alcohol-and-Drug-Abuse-Patient-Records-Regulation-and-the-HIPAA-Privacy-Rule/PHD1083.

- *The HIPAA Privacy and Security Rules—Frequently Asked Questions About the Disposal of Protected Health Information*, HHS, Office for Civil Rights (OCR), www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf.

- *The HIPAA Privacy Rule*, Justice and Health Connect, Substance Use and Mental Health Program at the Vera Institute of Justice, supported by the Department of Justice's (DOJ) Bureau of Justice Assistance, www.jhconnect.org/wp-content/uploads/2013/06/HIPAA-FINAL.pdf.

- The Unseen Provider (Video), New Jersey: Health Information Exchanges (HIEs) and the Camden County Jail, Community Oriented Correctional Health Services (COCHS), www.cochs.org/health_reform/hie_conf/unseen_provider.

  This video highlights the importance of linking jail systems to health information exchanges (HIEs) as a way of building connectivity between corrections and the community.

- *Tips, Tools, and Trends—Addressing the HIPAA in the Room*, NRC-CWDT, www.nrccwdt.org/wp-content/uploads/2012/04/TTT_HIPAA.pdf.

- Understanding Health Information Privacy, HHS, OCR, www.hhs.gov/ocr/privacy/hipaa/understanding/index.html.

Appendix I—Acknowledgments

A special thank-you is expressed to the following individuals and organizations for their assistance in the research, development, review, and pilot-testing of this privacy template.

Ms. Christina Abernathy
Senior Research Associate
Institute for Intergovernmental Research

Ms. Erin Boyar
Principal Planner
Planning and Research Unit
Rhode Island Department of Corrections

Maureen Boyle, Ph.D.
Health Information Technology
Substance Abuse and Mental Health Services Administration (SAMHSA)

Mr. Tony Bryant
Information Systems
Hampden County Sheriff's Department, Massachusetts

Mr. George Camp
Executive Director
Association of State Correctional Administrators (ASCA)

Ms. Bonnie Cosgrove
Reentry and Integrated Programs
Maryland Department of Public Safety and Correctional Services

Ms. Becki Goggins
Privacy and Data Specialist
Alabama Governor's Office

Ms. Diana Graski
Technology Department
National Center for State Courts (NCSC)

Superintendent John Kenney
Special Operations
Hampden County Sheriff's Department, Massachusetts

Ms. Mary Marcial
Association of State Correctional Administrators (ASCA)

Mr. Adam K. Matz
Research Associate
American Probation and Parole Association (APPA)
Council of State Governments (CSG)

Mr. Bob May
Assistant Director
Program and Technology Services
IJIS Institute

Ms. Patrice Miller
Substance Abuse
Maryland Department of Public Safety and Correctional Services

John Petrila, J.D., L.L.M.
College of Public Health—Health Policy and Management
University of South Florida

Mr. Tom Talbot
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

Mr. Carl Wicklund
Director
American Probation and Parole Association (APPA)
Council of State Governments (CSG)

Mr. John J. Wilson, Esquire
Senior Research Associate
Institute for Intergovernmental Research

Ms. Tammy Woodhams
Senior Staff Associate
National Criminal Justice Association