Ethics and HIPAA: What Mental Health Professionals Must Know

Material for Continuing Education

This course cannot be used to meet the GA Licensing Board's requirement of 5 hours of Ethics. Because it is an on-line course it can be used toward the 10 hrs. of on-line courses that counselors, social workers and Licensed Marriage and Family counselors are allowed to use as part of meeting the required 35 hours required to renew license.

This course counts as 3.5 ceu/clock hrs.

The following material was published in the public domain by the U.S. Department of Health and Human Services. Neither Karen McCleskey nor Dr. Karen McCleskey Workshops, Inc. is affiliated with the aforementioned department in any way.

The following information discusses and explains four areas of particular significance for mental health professionals regarding ethics and ethical decision making as related to understanding health information privacy:

1. HIPAA Administrative Simplification Statute and Rules:

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included **Administrative Simplification** provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).

HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).

OCR administers and enforces the Privacy Rule and the Security Rule.

Other HIPAA Administrative Simplification Rules are administered and enforced by the Centers for Medicare & Medicaid Services, and include:

- Transactions and Code Sets Standards
- Employer Identifier Standard
- National Provider Identifier Standard

http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

From http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

2. The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

3. The HIPAA Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information.

4. Confidentiality of Alcohol and Drug Abuse Patient Records examines the implications of the HIPAA Privacy Rule for Alcohol and Substance Abuse Programs.

---

2. SUMMARY OF THE HIPAA PRIVACY RULE

Contents

End Notes

OCR Privacy Rule Summary 1 Last Revised 05/03

Introduction

The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). [1] The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health

care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with all of its applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier for entities to review the complete requirements of the Rule, provisions of the Rule referenced in this summary are cited in notes at the end of this document. To view the entire Rule, and for other additional helpful information about how it applies, see the OCR website: http://www.hhs.gov/ocr/hipaa. In the event of a conflict between this summary and the Rule, the Rule governs.

Statutory & Regulatory Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the *Administrative Simplification* provisions.

HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within

three years of the passage of HIPAA. Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000.[2]

In March 2002, the Department proposed and released for public comment modifications to the Privacy Rule. The Department received over 11,000 comments. The final modifications were published in final form on August 14, 2002.[3] A text combining the final regulation and the modifications can be found at 45 CFR Part 160 and Part 164, Subparts A and E on the OCR website:

http://www.hhs.gov/ocr/hipaa.

Who is Covered by the Privacy Rule

The Privacy Rule, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities"). For help in determining whether you are covered, use the decision tool at: http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp.

Health Plans. Individual and group plans that provide or pay the cost of medical care are covered entities.[4] Health plans include health, dental, vision, and

prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of governmentfunded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) those programs whose principal activity is directly providing health care, such as a community health center,[5] or the making of grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance.

Health Care Providers. Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.[6] Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must

be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

Health Care Clearinghouses. *Health care clearinghouses* are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. [7] In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information.[8] Health care clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.

Business Associates

Business Associate Defined. In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.[9] Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. A covered entity can be the business associate of another covered entity.

Business Associate Contract. When a covered entity uses a contractor or other nonworkforce member to perform *"business associate"* services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections). In the business associate contract, a covered entity must impose specified written safeguards on the individually

identifiable health information used or disclosed by its business associates.[10] Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the Rule. Covered entities that have an existing written contract or agreement with business associates prior to October 15, 2002, which is not renewed or modified prior to April 14, 2003, are permitted to continue to operate under that contract until they renew the contract or April 14, 2004, whichever is first.[11] Sample business associate contract language is available on the OCR website at: http://www.hhs.gov/ocr/hipaa/contractprov.html.

What Information is Protected

Protected Health Information. The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "*protected health information (PHI)*."[12]

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,

 the provision of health care to the individual, or

 the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

De-Identified Health Information. There are no restrictions on the use or disclosure of de-identified health information.[14] De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.[15]

General Principle for Uses and Disclosures

Basic Principle. A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.[16]

Required Disclosures. A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.[17]

Permitted Uses and Disclosures

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care

Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and

(6) Limited Data Set for the purposes of research, public health or health care operations.[18] Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

(1) To the Individual. A covered entity may disclose protected health information to the individual who is the subject of the information.

(2) Treatment, Payment, Health Care Operations. A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.[19] A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship.

Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a

patient by one provider to another.[20]

Payment encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual[21] and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

Health care operations are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.[22]

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.[23]

Obtaining “consent” (written permission from individuals to use and disclose their protected health information for treatment, payment, and health care operations) is optional under the Privacy Rule for all covered entities.[24] The content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent.

(3) Uses and Disclosures with Opportunity to Agree or Object. Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

Facility Directories. It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual’s informal permission to list in its facility directory the individual’s name, general condition, religious affiliation, and location in the provider’s facility.[25] The provider may then disclose the individual’s condition and location in the facility to anyone asking for the individual by name, and also may disclose religious

affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.

For Notification and Other Purposes. A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care or payment for care. [26] This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death. In addition, protected health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

(4) Incidental Use and Disclosure. The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information

being shared was limited to the "minimum necessary," as required by the Privacy Rule.[27]

(5) Public Interest and Benefit Activities. The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes.[28] These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

Required by Law. Covered entities may use and disclose protected health information without individual authorization as *required by law* (including by

Public Health Activities. Covered entities may disclose protected health information to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and postmarketing surveillance; (3) individuals who may have contracted or been

exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.[30]

Victims of Abuse, Neglect or Domestic Violence. In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.[31]

Health Oversight Activities. Covered entities may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.[32]

Judicial and Administrative Proceedings. Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual

or a protective order are provided.[33]

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.[34]

Decedents. Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.[35]

Cadaveric Organ, Eye, or Tissue Donation. Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.[36]

Research. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge.[37] The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either: (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is

sought.[38] A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes (see discussion below).[39]

Serious Threat to Health or Safety. Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.[40]

Essential Government Functions. An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.[41]

Workers' Compensation. Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.[42] **(6) Limited Data Set**. A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.[43] A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.

Authorized Uses and Disclosures

Authorization. A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.[44] A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.[45]

An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's

authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes.

All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data. The Privacy Rule contains transition provisions applicable to authorizations and other express legal permissions obtained prior to April 14, 2003. [46]

Psychotherapy Notes[47]**.** A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions[48]:

- The covered entity who originated the notes may use them for treatment.
- A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as required by law.

Marketing. Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.[49] The Privacy Rule

carves out the following health-related activities from this definition of marketing:

 Communications to describe health-related products or services, or payment

for them, provided by or included in a benefit plan of the covered entity making the communication;

 Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan;

 Communications for treatment of the individual; and

 Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual.

Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. A covered entity must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity's provision of

promotional gifts of nominal value. No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition. An authorization for marketing that involves the covered entity's receipt of direct or indirect remuneration from a third party must reveal that fact.

Limiting Uses and Disclosures to the Minimum Necessary

Minimum Necessary. A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.[50] A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review

or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

Access and Uses. For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of

protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

Disclosures and Requests for Disclosures. Covered entities must establish and implement policies and procedures (which may be standard protocols) for *routine, recurring disclosures, or requests for disclosures,* that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria.

Reasonable Reliance. If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the covered entity's business associate, seeking the information to provide services to or for the covered entity; or (c) a researcher who provides the documentation or representation required by the Privacy Rule for research.

Notice and Other Individual Rights

Privacy Practices Notice. Each covered entity, with certain exceptions, must provide a notice of its privacy practices.[51] The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific

distribution requirements for direct treatment providers, all other health care providers, and health plans.

 Notice Distribution. A covered health care provider with a *direct treatment relationship* with individuals must deliver a privacy practices notice to patients starting April 14, 2003 as follows:

- Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery);
- By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and
- In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

Covered entities, whether *direct treatment providers* or *indirect treatment providers* (such as laboratories) or *health plans* must supply notice to anyone on request.[52] A covered entity must also make its notice electronically available on any web site it maintains for customer service or benefits information.

The covered entities in an *organized health care arrangement* may use a joint privacy practices notice, as long as each agrees to abide by the notice content with respect to the protected health information created or received in connection with participation in the arrangement.[53] Distribution of a joint notice by any covered entity participating in the organized health care arrangement at the first point that an OHCA member has an obligation to provide notice satisfies the distribution obligation of the other participants in the organized health care arrangement.

A health plan must distribute its privacy practices notice to each of its enrollees by its Privacy Rule compliance date. Thereafter, the health plan must give its notice to each new enrollee at enrollment, and send a reminder to every enrollee at least once every three years that the notice is available upon request. A health plan satisfies its distribution obligation by furnishing the notice to the "named insured," that is, the subscriber for coverage that also applies to spouses and dependents.

 Acknowledgement of Notice Receipt. A covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice.[54] The Privacy Rule does not prescribe any particular content for the acknowledgement. The provider must document the reason for any

failure to obtain the patient's written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

Access. Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's *designated record set*.[55] The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.[56] The Rule excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.[57] Covered entities may impose reasonable, cost-based fees for the cost of copying and postage.

Amendment. The Rule gives individuals the right to have covered entities amend

their protected health information in a designated record set when that information is

inaccurate or incomplete. [58] If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment.[59] If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity.

Disclosure Accounting. Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates.[60] The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date. The Privacy Rule does not require accounting for disclosures: (a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d)

pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities.

Restriction Request. Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death.[61] A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.[62]

Confidential Communications Requirements. Health plans and covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.[63] For example, an individual may request that the provider communicate with the individual through a designated address or

phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card.

Health plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the protected health information could endanger the individual. The health plan may not question the individual's statement of endangerment. Any covered entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

Administrative Requirements

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Privacy Policies and Procedures. A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.[64]

Privacy Personnel. A covered entity must designate a privacy official responsible

for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.[65]

Workforce Training and Management. Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).[66] A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions.[67] A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.[68]

Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.[69]

Data Safeguards. A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.[70] For example, such safeguards might include shredding documents containing protected health information before

discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes.

Complaints. A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule.[71] The covered entity must explain those procedures in its privacy practices notice.[72] Among other things, the covered entity must identify to whom individuals can submit complaints to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS.

Retaliation and Waiver. A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.[73] A covered entity may not

require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.[74]

Documentation and Record Retention. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.[75]

Fully-Insured Group Health Plan Exception. The only administrative obligations with which a fully-insured group health plan that has no more than enrollment data and summary health information is required to comply are the (1) ban on retaliatory acts and waiver of individual rights, and (2) documentation requirements with respect to plan documents if such documents are amended to provide for the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO that services the group health plan.[76]

Organizational Options

The Rule contains provisions that address a variety of organizational issues that may affect the operation of the privacy protections.

Hybrid Entity. The Privacy Rule permits a covered entity that is a single legal entity and that conducts both covered and non-covered functions to elect to be a "hybrid entity."[77] (The activities that make a person or organization a covered entity are its "covered functions."[78]) To be a hybrid entity, the covered entity must designate in writing its operations that perform covered functions as one or more "health care components." After making this designation, most of the requirements of the Privacy Rule will apply only to the health care components. A covered entity that does not make this designation is subject in its entirety to the Privacy Rule.

Affiliated Covered Entity. Legally separate covered entities that are affiliated by

common ownership or control may designate themselves (including their health care components) as a single covered entity for Privacy Rule compliance.[79] The designation must be in writing. An affiliated covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.

Organized Health Care Arrangement. The Privacy Rule identifies relationships in which participating covered entities share protected health information to manage and benefit their common enterprise as "organized health care arrangements."[80] Covered entities in an organized health care arrangement can share protected health information with each other for the arrangement's joint health care operations.[81]

Covered Entities With Multiple Covered Functions. A covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.[82] The covered entity may not use or disclose the protected health information of an individual who receives services from one covered function (e.g., health care provider) for another covered function (e.g., health plan) if the individual is not involved with the other function.

Group Health Plan disclosures to Plan Sponsors. A group health plan and the health insurer or HMO offered by the plan may disclose the following protected

health information to the “plan sponsor”—the employer, union, or other employee organization that sponsors and maintains the group health plan[83]:

 Enrollment or dis-enrollment information with respect to the group health plan or a health insurer or HMO offered by the plan.

 If requested by the plan sponsor, summary health information for the plan sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend, or terminate the group health plan. “Summary health information” is information that summarizes claims history, claims expenses, or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five digit zip code (though it need not qualify as de-identified protected health information).

 Protected health information of the group health plan’s enrollees for the plan sponsor to perform plan administration functions. The plan must receive certification from the plan sponsor that the group health plan document has been amended to impose restrictions on the plan sponsor’s use and disclosure of the protected health information. These restrictions must include the representation that the plan sponsor will not use or disclose the protected health information for any employment-related action or decision or in

connection with any other benefit plan.

Other Provisions:

Personal Representatives and Minors

Personal Representatives. The Privacy Rule requires a covered entity to treat a *"personal representative"* the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule.[84] A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual.

Special case: Minors. In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these

situations, the Privacy Rule defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment.

State Law

Preemption. In general, State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply.[85] "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.[86] The Privacy Rule provides exceptions to the general rule of federal preemption for contrary State laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain health

plan reporting, such as for management or financial audits.

Exception Determination. In addition, preemption of a contrary State law will not occur if HHS determines, in response to a request from a State or other entity or person, that the State law:

 Is necessary to prevent fraud and abuse related to the provision of or payment for health care,

 Is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

 Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

Enforcement and Penalties for Noncompliance

Compliance. Consistent with the principles for achieving compliance provided in the Rule, HHS will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Rule.[87] The Rule provides processes for persons to file complaints with HHS, describes the

responsibilities of covered entities to provide records and compliance reports and to cooperate with, and permit access to information for, investigations and compliance reviews.

Civil Money Penalties. HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement.[88] That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

Criminal Penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment.[89] The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.

Compliance Dates

Compliance Schedule. All covered entities, except "small health plans," must be compliant with the Privacy Rule by April 14, 2003.[90] Small health plans, however, have until April 14, 2004 to comply.

Small Health Plans. A health plan with annual receipts of not more than $5 million is a small health plan.[91] Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 Code of Federal Regulations (CFR) 121.104 to calculate annual receipts. Health plans that do not report receipts to the Internal Revenue Service (IRS), for example, group health plans regulated by the Employee Retirement Income Security Act 1974 (ERISA) that are exempt from filing income tax returns, should use proxy measures to determine their annual receipts.[92]

Copies of the Rule & Related Materials

The entire Privacy Rule, as well as guidance and additional materials, may be found by going to http://www.hhs.gov/ocr/hipaa.

End Notes

[1] Pub. L. 104-191.

[2] 65 FR 82462.

[3] 67 FR 53182.

[4] 45 C.F.R. §§ 160.102, 160.103.

[5] Even if an entity, such as a community health center, does not meet the definition of a health plan, it may, nonetheless, meet the definition of a health care provider, and, if it transmits health information in electronic form in connection with the transactions for which the Secretary of HHS has adopted standards under HIPAA, may still be a covered entity.

[6] 45 C.F.R. §§ 160.102, 160.103; *see* Social Security Act § 1172(a)(3), 42 U.S.C. § 1320d-1(a)(3). The transaction standards are established by the HIPAA Transactions Rule at 45 C.F.R. Part 162.

[7] 45 C.F.R. § 160.103.

[8] 45 C.F.R. § 164.500(b).

[9] 45 C.F.R. § 160.103.

[10] 45 C.F.R. §§ 164.502(e), 164.504(e).

[11] 45 C.F.R. § 164.532

[12] 45 C.F.R. § 160.103.

[13] 45 C.F.R. § 160.103

[14] 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

[15] The following identifiers of the individual or of relatives, employers, or household members of

the individual must be removed to achieve the “safe harbor” method of de-identification: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census (1) the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses: (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and ® any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met. In addition to the removal of the above-stated identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information. 45 C.F.R. § 164.514(b).

[16] 45 C.F.R. § 164.502(a).

[17] 45 C.F.R. § 164.502(a)(2).

[18] 45 C.F.R. § 164.502(a)(1).

[19] 45 C.F.R. § 164.506(c).

[20] 45 C.F.R. § 164.501.

[21] 45 C.F.R. § 164.501.

[22] 45 C.F.R. § 164.501.

[23] 45 C.F.R. § 164.508(a)(2)

[24] 45 C.F.R. § 164.506(b).

[25] 45 C.F.R. § 164.510(a).

[26] 45 C.F.R. § 164.510(b).

[27] 45 C.F.R. §§ 164.502(a)(1)(iii).

[28] *See* 45 C.F.R. § 164.512.

[29] 45 C.F.R. § 164.512(a).

[30] 45 C.F.R. § 164.512(b).

[31] 45 C.F.R. § 164.512(a), (c).

[32] 45 C.F.R. § 164.512(d).

[33] 45 C.F.R. § 164.512(e).

[34] 45 C.F.R. § 164.512(f).

[35] 45 C.F.R. § 164.512(g).

[36] 45 C.F.R. § 164.512(h).

[37] The Privacy Rule defines research as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." 45 C.F.R. § 164.501.

[38] 45 C.F.R. § 164.512(i).

[39] 45 CFR § 164.514(e).

[40] 45 C.F.R. § 164.512(j).

[41] 45 C.F.R. § 164.512(k).

[42] 45 C.F.R. § 164.512(l).

[43] 45 C.F.R. § 164.514(e). A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses: (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; (xvi) Full face photographic images and any comparable images. 45 C.F.R. § 164.514(e)(2).

[44] 45 C.F.R. § 164.508.

[45] A covered entity may condition the provision of health care solely to generate protected health

information for disclosure to a third party on the individual giving authorization to disclose the

information to the third party. For example, a covered entity physician may condition the provision of a physical examination to be paid for by a life insurance issuer on an individual's authorization to disclose the results of that examination to the life insurance issuer. A health plan may condition enrollment or benefits eligibility on the individual giving authorization, requested before the individual's enrollment, to obtain protected health information (other than psychotherapy notes) to determine the individual's eligibility or enrollment or for underwriting or risk rating. A covered health care provider may condition treatment related to research (e.g., clinical trials) on the individual giving authorization to use or disclose the individual's protected health information for the research. 45 C.F.R. 508(b)(4).

[46] 45 CFR § 164.532.

[47] "Psychotherapy notes" means 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 of the individual's medical record. Psychotherapy notes excludes 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, the treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R. § 164.501.

[48] 45 C.F.R. § 164.508(a)(2).

[49] 45 C.F.R. §§ 164.501 and 164.508(a)(3).

[50] 45 C.F.R. §§ 164.502(b) and 164.514 (d).

[51] 45 C.F.R. §§ 164.520(a) and (b). A group health plan, or a health insurer or HMO with respect to the group health plan, that intends to disclose protected health information (including enrollment data or summary health information) to the plan sponsor, must state that fact in the notice. Special statements are also required in the notice if a covered entity intends to contact individuals about health-related benefits or services, treatment alternatives, or appointment reminders, or for the covered entity's own fundraising.

[52] 45 C.F.R. § 164.520(c).

[53] 45 C.F.R. § 164.520(d).

[54] 45 C.F.R. § 164.520(c).

[55] 45 C.F.R. § 164.524.

[56] 45 C.F.R. § 164.501.

[57] A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed by a licensed health care professional (who is designated by the covered entity and who did not participate in the original decision to deny), when a licensed health care professional has determined, in the exercise of professional judgment, that: (a) the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; (b) the protected health information makes reference to another person (unless such other person is a health care provider) and the access requested is reasonably likely to cause substantial harm to such other person; or (c) the request for access is made by the individual's personal

representative and the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

A covered entity may deny access to individuals, without providing the individual an opportunity for review, in the following protected situations: (a) the protected health information falls under an exception to the right of access; (b) an inmate request for protected health information under certain circumstances; (c) information that a provider creates or obtains in the course of research that includes treatment for which the individual has agreed not to have access as part of consenting

to participate in the research (as long as access to the information is restored upon completion of the research); (d) for records subject to the Privacy Act, information to which access may be denied under the Privacy Act, 5 U.S.C. § 552a; and (e) information obtained under a promise of confidentiality from a source other than a health care provider, if granting access would likely reveal the source. 45 C.F.R. § 164.524.

58 45 C.F.R. § 164.526.

59 Covered entities may deny an individual's request for amendment only under specified circumstances. A covered entity may deny the request if it: (a) may exclude the information from access by the individual; (b) did not create the information (unless the individual provides a reasonable basis to believe the originator is no longer available); (c) determines that the information is accurate and complete; or (d) does not hold the information in its designated record set. 164.526(a)(2).

60 45 C.F.R. § 164.528.

[61] 45 C.F.R. § 164.522(a).

[62] 45 C.F.R. § 164.522(a). In addition, a restriction agreed to by a covered entity is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

[63] 45 C.F.R. § 164.522(b).

[64] 45 C.F.R. § 164.530(i).

[65] 45 C.F.R. § 164.530(a).

[66] 45 C.F.R. §160.103.

[67] 45 C.F.R. § 164.530(b).

[68] 45 C.F.R. § 164.530(e).

[69] 45 C.F.R. § 164.530(f).

[70] 45 C.F.R. § 164.530(c).

[71] 45 C.F.R. § 164.530(d).

[72] 45 C.F.R. § 164.520(b)(1)(vi).

[73] 45 C.F.R. § 164.530(g).

[74] 45 C.F.R. § 164.530(h).

[75] 45 C.F.R. § 164.530(j).

[76] 45 C.F.R. § 164.530(k).

[77] 45 C.F.R. §§ 164.103, 164.105.

[78] 45 C.F.R. § 164.103.

[79] 45 C.F.R. §164.105. Common ownership exists if an entity possesses an ownership or equity

interest of five percent or more in another entity; common control exists if an entity has the direct or indirect power significantly to influence or direct the actions or policies of another entity. 45 C.F.R. §§ 164.103.

[80] The Privacy Rule at 45 C.F.R. § 160.103 identifies five types of organized health care arrangements:

- A clinically-integrated setting where individuals typically receive health care from more than one provider.
- An organized system of health care in which the participating covered entities hold themselves out to the public as part of a joint arrangement and jointly engage in

The following material was published in the public domain by the U.S. Department of Health and Human Services. Neither Karen McCleskey nor Dr. Karen McCleskey Workshops, Inc. is affiliated with the aforementioned department in any way.

The source is:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

---

3. The HIPAA Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The

Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf

---

4. The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule:

Implications For Alcohol and Substance Abuse Programs

The following material was published in the public domain by the U.S. Department of Health and Human Services. Neither Karen McCleskey nor Dr. Karen McCleskey Workshops, Inc. is affiliated with the aforementioned department in any way.

The following information is from the U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES Substance Abuse and Mental Health Services Administration Center for Substance Abuse Treatment www.samhsa.gov

The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs

Introduction

In the early 1970's, Congress recognized that the stigma associated with substance abuse and fear of prosecution deterred people from entering treatment and enacted legislation that gave patients a right to confidentiality. For the almost three decades since the Federal confidentiality regulations (42 CFR Part 2 or Part 2) were issued, confidentiality has been a cornerstone practice for substance abuse treatment programs across the country.

In December, 2000, the Department of Health and Human Services (HHS) issued the "Standards for Privacy of Individually Identifiable Health Information" final rule (Privacy Rule), pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR Parts 160 and 164, Subparts A and E.[1] Substance abuse treatment programs that are subject to HIPAA must comply with the Privacy Rule.[2][3] Substance abuse treatment programs that already are complying with Part 2 should not have a difficult time complying with the Privacy Rule, as it parallels the requirements of Part 2 in many areas. Programs subject to both sets of rules must comply with both, unless there is a conflict between them. Generally, this will mean that substance abuse treatment programs should continue to follow the Part 2 regulations. In some instances, programs will have to establish new policies and procedures or alter existing policies and practices. In the event a program identifies a conflict between the rules, it should notify the Substance Abuse and Mental Health Services Administration of HHS immediately for assistance in resolving the conflict.

This guidance is for substance abuse treatment programs that are subject to and already complying with the confidentiality requirements of Part 2.[4] It explains which programs must also comply with the Privacy Rule and outlines what compliance will require. The guidance is not a legal opinion. To comply with the Privacy Rule, programs should apply this guidance to their individual situations; programs may also want to call upon State agencies, provider organizations and legal counsel for assistance in establishing and implementing the practices and policy changes required by the Privacy Rule.

[1] In August 2002, HHS adopted modifications to the Privacy Rule. [2] The compliance date for the Privacy Rule was April 14, 2003. However, small health plans, as defined by the Privacy Rule, are not required to be in compliance until April 14, 2004. [3] This guidance applies to substance abuse treatment programs that are also covered entities as defined by the Privacy Rule. Programs should seek legal counsel for assistance in determining whether they are covered entities. [4] The Part 2 regulations apply to substance abuse treatment "programs" as defined by 42 CFR §2.11 that are "federally assisted" as defined by 42 CFR §2.12(b).

I. Applicability

A. Programs to which the Privacy Rule applies

The Privacy Rule applies to "covered entities" which are health plans, health care clearinghouses and health care providers[5] who transmit health information in electronic form (*i.e.*, via computer-based technology) in connection with transactions for which HHS has adopted a HIPAA standard in 45 CFR Part 162. See 45 CFR §160.103. HIPAA transactions that a substance abuse treatment program[6] might engage in include:

- Submission of claims to health plans
- Coordination of benefits with health plans
- Inquiries to health plans regarding eligibility, coverage or benefits or status of health care claims
- Transmission of enrollment and other information related to payment to health plans
- Referral certification and authorization (*i.e.*, requests for review of health care to obtain an authorization for providing health care or requests to obtain authorization for referring an individual to another health care provider)

If a substance abuse treatment program transmits health information electronically in connection with one or more of these Part 162 transactions, then it must comply with the Privacy Rule. Part 162 may be amended in the future to cover additional transactions.[7]

B. Information that is protected under Part 2 and the Privacy Rule

Part 2 protects any and all information that could reasonably be used to identify an individual and requires that disclosures be limited to the information necessary to carry out the purpose of the disclosure. See 42 CFR §§2.11 and 2.13(a). Under the Privacy Rule, a program may not use or disclose "protected health information" (PHI) except as permitted or required by the Rule.[8] See 45 CFR §164.502(a). Neither rule applies to information that has been de-identified.[9]

[5] The Privacy Rule generally defines a health care provider to include a person or organization who furnishes, bills or is paid for health care in the normal course of business, which would include substance abuse treatment programs. [6] A substance abuse treatment program is defined as an individual or entity that provides alcohol or drug abuse diagnosis, treatment or referral. For the purposes of this document, the term "program" includes both individual substance abuse providers and substance abuse provider organizations. [7] Neither Part 2 nor the Privacy Rule protects employment records held by a program in its role as employer. Note that while 42 CFR Part 2 arguably applies to substance abuse patient records covered by the Family Educational Rights and Privacy Act (FERPA) (20 USC §1232g; 34 CFR Part 99), the Privacy Rule does not. [8] PHI is defined as individually identifiable health information held or transmitted by a covered entity or its "business associate," with limited exceptions. See 45 CFR §160.103. [9] The Privacy Rule includes numerous elements that make information identifiable, such as, but not limited to, information regarding employers, relatives and household members.

The Privacy Rule permits programs to assign a code or other means of record identification to allow information that has been de-identified to be re-identified, as provided in 45 CFR §164.514(c).

The two regulations have some differences in the definition of what information is protected. For instance, the Privacy Rule treats medical record numbers as PHI, subject to all the same requirements as other PHI. Part 2 would permit a program to disclose a medical record number because the regulation does not apply to "a number assigned to a patient by a program, if that number does not consist of, or contain numbers . . . which could be used to identify a patient with reasonable accuracy and speed from sources external to the program." See 42 CFR §2.11. Programs subject to both rules must follow the Privacy Rule's protection of a medical record number.

C. When protections begin for someone seeking substance abuse treatment

Part 2 protects all information about any person who has applied for or been given diagnosis or treatment for alcohol or drug abuse at a federally assisted program. See 42 CFR §2.11 (definition of a "patient"). Information is subject to the Privacy Rule if it is individually identifiable information created, received, or maintained by the covered entity. Former patients and deceased patients are protected under both Part 2 and the Privacy Rule. See 42 CFR §§2.11 and 2.15 and 45 CFR §§164.501 and 164.502(f). Programs should generally continue to follow Part 2, but note that if PHI is received prior to a patient applying to a program, under the Privacy Rule, such information is protected.

II. How the Privacy Rule affects disclosures of information

A. The General Rule

The "general rules" established by Part 2 and the Privacy Rule regarding uses and disclosures of patient health information are very different.[10]

Substance abuse treatment programs must comply with both rules. Generally, this will mean that they will continue to follow Part 2's general rule and not disclose information unless they can obtain consent or point to an exception to that rule that specifically permits the disclosure. Programs must then make sure that the disclosure is also permissible under the Privacy Rule.

B. When disclosures are permitted

identifiable information under Part 2. Such information should be protected consistent with the Privacy Rule requirements. [10] Part 2 uses the term "disclosure" to cover what the Privacy Rule refers to as "uses" and "disclosures." See the definition of these terms in 45 CFR §160.103. Some Privacy Rule provisions differ for "uses" and "disclosures." For convenience, we generally use the Part 2 term "disclosure" throughout to encompass both uses and disclosures under the Privacy Rule. In some instances, however, specific uses or disclosures are discussed.

Programs may not use or disclose any information about any patient unless the patient has consented in writing (on a form that meets the requirements established by the regulations) or unless another very limited exception specified in the regulations applies. Any disclosure must be limited to the information necessary to carry out the purpose of the disclosure.

The Privacy Rule

The Privacy Rule permits uses and disclosures for "treatment, payment and health care operations" as well as certain other disclosures without the individual's prior written authorization. Disclosures not otherwise specifically permitted or required by the Privacy Rule must have an authorization that meets certain requirements. With certain exceptions, the Privacy Rule generally requires that uses and disclosures of PHI be the minimum necessary for the intended purpose of the use or disclosure.

Substance abuse treatment programs most often make disclosures after a patient has signed a consent form that meets the requirements of 42 CFR §2.31. Note that a disclosure under Part 2 includes the acknowledgment that someone has applied to or is enrolled in the program, and thus is only permitted if the patient has signed a consent form (or another of the regulations' narrow exceptions applies). See 42 CFR §§2.11 and

2.13. A Part 2 consent form must include the following elements:

- Name or general designation of the program or person permitted to make the disclosure;
- Name or title of the individual or name of the organization to which disclosure is to be made;
- Name of the patient;
- Purpose of the disclosure;
- How much and what kind of information is to be disclosed;
- Signature of patient (and, in some States, a parent or guardian);
- Date on which consent is signed;
- Statement that the consent is subject to revocation at any time except to the extent that the program has already acted on it; and
- Date, event, or condition upon which consent will expire if not previously revoked.

[11] This document uses the term "consent" when referring to any written permission provided by a patient for the use or disclosure of identifiable health information. The Privacy Rule uses the term "authorization" for certain permissions, and also permits, but does not require, programs to obtain "consent" for the use and disclosure of PHI for purposes of treatment, payment, or health care operations. 5

When programs operating under Part 2 disclose information pursuant to a consent form, they must include a written statement that the information cannot be redisclosed. See 42 CFR §2.32.

The core required elements for the Privacy Rule written authorization are similar to those of Part 2. However, to comply with the Privacy Rule authorization requirements, the Part 2 consent must also contain a statement reflecting the ability or inability of the substance abuse treatment program to condition treatment on whether the patient signs the form as described in 45 CFR §164.508(c)(2)(ii). In addition, the consent may be signed by a personal representative, and if so, must include a description of such representative's authority to act for the patient. See 45 CFR §164.508(c)(1)(vi). Finally, the consent must be written in plain language. See 45 CFR §164.508(c)(3).

The requirements above must be met with respect to the Part 2 consent form when the purpose of the disclosure is *not* for "treatment, payment or health care operations" or for any other permitted or required disclosure under the Privacy Rule. See 45 CFR §164.502(a).[12] The statements would have to be added when the consent form authorizes a program to make a disclosure for which an authorization is required under the Privacy Rule, e.g., those disclosures addressed by 45 CFR §164.508.

The Privacy Rule imposes three additional steps programs must take when disclosing information pursuant to a patient's written consent:

- Programs must ensure that the consent complies with the applicable requirements of 45 CFR §164.508.
- Programs must give patients a copy of the signed form (45 CFR §164.508(c)(4)).
- Programs must keep a copy of each signed form for six (6) years from its expiration date (45 CFR §164.508(b)(6)).

Therefore, substance abuse treatment programs should generally continue to use the consent form for disclosures subject to Part 2. If the Privacy Rule requires authorization for the disclosures, the substance abuse treatment program may use the Part 2 consent form with additional elements required by the Privacy Rule as listed above.

Minors

[12] See the Privacy Rule's definitions of "treatment," "payment," and "health care operations" at 45 CFR §164.501. When a substance abuse treatment program obtains information about a patient from a school, relatives, health care providers and health plans for treatment or payment activities, when it refers a patient to other providers and services and when it coordinates care with other health care providers, it almost always makes an implicit disclosure that the patient has applied for or has received alcohol or drug abuse treatment services and thus the program is required to treat these contacts as disclosures and obtain patient consent prior to such contact. In most of these instances, the disclosure from the program is for treatment purposes and the additional Privacy Rule statements would not have to be added to the consent forms. Note that programs may add the Privacy Rule statements in all circumstances, and programs may find it more convenient to use only one kind of consent form.

The Privacy Rule defers to requirements in other applicable laws regarding the use or disclosure of health information regarding minors and, thus, does not change the rules in Part 2 regarding minors and consent. See 45 CFR §164.502(g). A minor must always sign the consent form for a program to release information even to his or her parent or guardian (42 CFR §2.14).[13] Some States require programs to obtain parental permission before providing treatment to a minor. In these States only, programs must get the signatures of both the minor and a parent, guardian, or other person legally responsible for the minor (42 CFR §2.14(c)(2)).

Revocation of Consent

Part 2 permits a patient to revoke consent orally (see 42 CFR §2.31(a)(8)); the Privacy Rule requires written revocation of an authorization (45 CFR §164.508(b)(5)). Substance abuse treatment programs must continue to honor verbal revocations but may want to obtain written revocation when possible or at a minimum document the revocation in the patient's record. Both Part 2 and the Privacy Rule allow the program to make a disclosure for services already rendered in reliance on a signed consent or authorization form. See 42 CFR §2.31(a)(8) and 45 CFR §164.508(b)(5)(i).

2. Other permissible disclosures under Part 2

Substance abuse treatment programs are accustomed to complying with Part 2's general rule prohibiting disclosure, unless the patient has consented in writing or the disclosure falls within one of the regulations' limited exceptions (*e.g.*, child abuse reporting, medical emergencies). In some instances, the Privacy Rule does not require a change in these practices. In others, the Privacy Rule will require some modification of programs' practices.

a. When little or no changes may be needed

Programs should generally continue to follow the rules in Part 2 regarding:

i. Internal program communications

Both Part 2 and the Privacy Rule allow for communications within programs on a "need to know" basis. Part 2 requires that the communication of information within the program (or to an entity with direct administrative control over the program)[14]

[13] The only exception to this rule is when the program director determines that a minor applying for services lacks capacity for rational choice and that the minor applicant's situation poses a substantial threat to life or physical well being of the minor or any other person that may be reduced by communicating relevant facts to the minor's parent or guardian. See 42 CFR §2.14(d).

[14] In applying the Privacy Rule, programs should consider whether the program and the entity with "direct administrative control" over the program are two separate legal entities. If they are two separate legal entities, PHI flowing between the program and the other entity will generally be governed by the Privacy Rule's requirements regarding "disclosure" rather than "use" of PHI. However, the Privacy Rule recognizes that health care providers may have different organizational arrangements and has established different rules to reflect such arrangements. See the Privacy Rule's provisions regarding hybrid entities 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 alcohol or drug abuse. See 42 CFR §2.12(c)(3). Similarly, the Privacy Rule requires programs to identify the staff persons or classes of persons in its workforce who need access to PHI, the categories of PHI they need access to, and any conditions appropriate to such access. See 45 CFR §164.514(d)(2)(i). The program must then make reasonable efforts to limit access of such persons or classes of persons to PHI based on these determinations. See 45 CFR §164.514(d)(2)(ii). Substance abuse treatment programs subject to the

Privacy Rule will have to establish written policies to comply with the minimum necessary requirement of the Privacy Rule, although in practice, the programs should be able to operate as they have under Part 2 in this regard.

ii. Crimes on program premises or against program personnel

Part 2 permits programs to disclose limited information to law enforcement officers. Such disclosures must be directly related to crimes and threats to commit crimes on program premises or against program personnel and must be limited to the circumstances of the incident and the patient's status, name, address and last known whereabouts. See 42 CFR §2.12(c)(5). The Privacy Rule permits programs to disclose to law enforcement officials PHI that the program believes in good faith constitutes evidence of a crime that occurred on the program's premises. See 45 CFR §164.512(f)(5). It also permits any member of the program's staff who is the victim of a crime to report certain information about the suspected perpetrator to law enforcement officials. See 45 CFR §164.502(j)(2). Programs should continue to follow the rules established by Part 2.

iii. Child abuse reporting

Part 2 permits programs to comply with State laws that require the reporting of child abuse and neglect. See 42 CFR §2.12(c)(6). The Privacy Rule also permits such reporting. See 45 CFR §164.512(b)(1)(ii). However, Part 2 limits programs to making only an initial report; it does not allow programs to respond to follow-up requests for information or to subpoenas, unless the patient has signed a consent form or a court has issued an order that complies with the rule (see "Subpoenas and court-ordered disclosures," below). Programs should continue to follow the rules established by Part 2.

iv. Medical emergencies

Part 2 allows patient-identifying information to be disclosed to medical personnel who have a need for the information about a patient for the purpose of treating a condition which poses an immediate threat to the health of any individual.

(45 CFR §164.105(a) and (c)), affiliated covered entities (45 CFR §164.105(b) and (c)), and organized health care arrangements (OHCAs) (45 CFR §160.103 (definition of "business associate" and "OHCA"), 45 CFR §164.506(c)(5), and 45 CFR §164.520(d)).

Immediate medical intervention. See 42 CFR §2.51. A program can disclose information only to medical personnel and must limit the amount of information to that which is necessary to treat the emergency medical condition. Immediately following the disclosure, the program must document the following in the patient's records:

- The name and affiliation of the medical personnel to whom disclosure was made;
- The name of the individual making the disclosure;
- The date and time of the disclosure; and
- The nature of the emergency.

These practices are not affected by the Privacy Rule.

v. Subpoenas and court-ordered disclosures

Part 2 permits programs to release information in response to a subpoena if the patient signs a consent permitting release of the information requested in the subpoena. When the patient does not consent, Part 2 prohibits programs from releasing information in response to a subpoena, unless a court has issued an order that complies with the rule. See 42 CFR Part 2, Subpart E. Subpart E sets out the procedure the court must follow, the findings it must make, and the limits it must place on any disclosure it authorizes.

The Privacy Rule permits a program to disclose PHI pursuant to a subpoena without a prior written authorization, if it receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to ensure that the individual has been given notice of the request for PHI and the opportunity to object, or reasonable efforts have been made to secure a qualified protective order. See 45 CFR §164.512(e)(1)(ii). The Privacy Rule has different requirements regarding court orders, but programs can comply with both Part 2 and the Privacy Rule by continuing to follow the Part 2's court order requirements. Unless the disclosure requires authorization under the Privacy Rule, the Part 2 consent form can be used.

b. When some change is required

i. Disclosures that do not reveal patient-identifying information

Part 2 permits a substance abuse treatment program to disclose information about a patient if the disclosure does not identify the patient as an alcohol or drug abuser or as someone who has applied for or received substance abuse assessment or treatment services. See 42 CFR §§2.11 and 2.12(a). This allows a program that is part of a larger entity, such as a hospital, to disclose information about a patient so long as it does not explicitly or implicitly disclose the fact that the patient is an alcohol or drug abuser. For example, a program that is part of a hospital could disclose to a public health department that a named patient has TB by identifying itself only as part of the hospital and not as a substance abuse treatment program and by taking care not to mention that the patient is in substance abuse treatment.

Many programs that are part of larger entities are accustomed to using this exception in Part 2 to gather information about patients from, for example, other health care providers, schools, and employers, or to refer patients to other providers.[15] Some of these practices by programs that are part of larger entities will continue to be permissible under the Privacy Rule, which does not require patients to authorize disclosures for purposes of treatment, payment or health care operations. The Privacy Rule also permits programs to share information about an individual's treatment or payment related to the individual's health care with persons involved in the individual's care. See 45 CFR §164.510(b).

The Privacy Rule also allows for certain disclosures to be made without authorization that are not for treatment, payment or health care operations. See 45 CFR §164.512. For example, the Privacy Rule permits a program to disclose, without the patient's prior authorization, to a public health department that the patient has TB when the health department is authorized to collect such information. However, any program that is accustomed to making "non-patient identifying" disclosures of information that do not identify the subject as a substance abuser and that are not for treatment purposes should consult the Privacy Rule directly to determine whether those disclosures continue to be permissible.

Part 2 does not permit freestanding programs to make inquiries about patients or refer patients to other providers without written consent. The Privacy Rule does not change this prohibition.

ii. Disclosures to agencies that provide services to programs

Disclosures to Qualified Service Organizations

Both Part 2 and the Privacy Rule recognize that substance abuse treatment programs sometimes need to disclose information about patients to persons or agencies that provide services to the program, such as legal or accounting services. The Part 2 regulations call such service providers "qualified service organizations" and permit programs to sign "qualified service organization agreements" (QSOAs) allowing them to disclose patient-identifying information needed by the organization to provide services to the program. See 42 CFR §2.12(c)(4). In the agreements, the outside service providers acknowledge that in receiving, storing, processing or otherwise dealing with patients' records they are fully bound by 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 Part 2 regulations.

Under the Privacy Rule, such outside service providers are "business associates" of the substance abuse treatment program and the program must have a business associate agreement with the business associate in order to share PHI needed by the organization

[15] As noted above, when a program makes an inquiry about, or refers, a patient, it is often making an implicit disclosure that the patient is in substance abuse treatment.

to provide services (see 45 CFR §§160.103 and 164.502(e)).[16] The Privacy Rule has different requirements regarding the content of the business associate contract (the HHS Office for Civil Rights has published sample contract language). See 67 Federal Register 53264 (August 14, 2002).

Substance abuse treatment programs must meet the requirements of both Part 2 and the Privacy Rule if they are going to continue to share information with lawyers, accountants and others that provide services to the program.

Transition Provisions: The Privacy Rule permits programs to continue to use current contracts with service providers until April 14, 2004, if the contract existed prior to October 15, 2002, and the contract is not subsequently renewed or modified. Any contract that is renewed or modified after October 15, 2002, must comply with the business associate contract requirements. See 45 CFR §164.532(d).

Disclosures to accreditation bodies

Part 2 permits disclosures to accreditation bodies such as the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) under either the QSO provision or the "audit and evaluation" exception, discussed below. The Privacy Rule, however, considers accreditation bodies business associates conducting health care operations on behalf of the covered entity. See 45 CFR §§160.103; 164.501. Substance abuse treatment programs subject to the Privacy Rule who undergo accreditation will have to sign business associate contracts with accreditation organizations. Additionally, substance abuse treatment programs must comply with Part 2, either by ensuring that the business associate contract contains all the requirements of a QSOA or by fulfilling the mandates of the audit and evaluation provisions.

iii. Audit and evaluation

Both Part 2 and the Privacy Rule permit programs to disclose patient-identifying information to qualified persons who are conducting an audit or evaluation of the program, without patient consent, provided that certain safeguards are met. The Privacy Rule requires that uses and disclosures be limited to the minimum necessary to accomplish the audit or evaluation. Each rule has its own additional requirements. Substance abuse treatment programs subject to both Part 2 and the Privacy Rule must combine those requirements. Three options result:

- If the audit or evaluation is conducted by a program or its employees, it is permissible under both sets of regulations; no patient consent or authorization is required. See 42 CFR §2.12(c)(3) and 45 CFR §164.502(a)(1)(ii).

[16] A memorandum of understanding would generally be used between government entities rather than a business associate contract.

- If the audit or evaluation is conducted by a "health oversight agency,"[17] the program may disclose patient-identifying information so long as the health oversight agency makes the written commitments required by 42 CFR §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 program, it must agree in writing to abide by the requirements of 42 CFR §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 a business associate contract with the auditor or evaluator that satisfies the requirements of both the Privacy Rule and Part 2 by incorporating either the necessary QSO agreement requirements (as discussed above in II.B.2.b.ii) or the appropriate provisions of 42 CFR §2.53.

iv. Research

The Part 2 regulations and the Privacy Rule have different requirements for disclosures of health information to researchers. See 42 CFR §2.52 and 45 CFR §164.512(i). This will be the subject of additional guidance.

III. Other Changes Required by the Privacy Rule[18]

A. Patient Notice/Notice of Privacy Practices

Part 2 requires that programs notify patients that Federal law and regulations protect the confidentiality of alcohol and drug abuse patient records and give them a written summary of the regulations' requirements. See 42 CFR §2.22. The Privacy Rule requires that patients be given a notice of the program's privacy practices as well as their rights under the Privacy Rule. See 45 CFR §164.520. Programs subject to both rules can combine their requirements into a single notice.

1. Notice content

Accordingly, the combined notice must contain all the elements required by 42 CFR §2.22, and in addition, contain the following:

[17] Under the Privacy Rule, a "health oversight agency" is an agency or authority or 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 (45 CFR §164.501). Disclosures to health oversight agencies when an individual is the subject of the investigation are prohibited under certain

circumstances by the Privacy Rule (45 CFR §164.512(d)(2)).[18] This last section addresses issues on which Part 2 is largely silent. Thus, these can be seen as new requirements imposed by the Privacy Rule to which programs now must adhere.

- A statement, prominently displayed stating: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY;”
- • A description in sufficient detail of the types of uses and disclosures that the program may make without the patient’s consent or authorization.[19] For substance abuse treatment programs, these would include uses and disclosures:
  - o In connection with treatment, payment or health care operations (include at least one example of each);
  - o To qualified service organizations or business associates who provide services to the program’s treatment, payment or health care operations;
  - o In medical emergencies;
  - o Authorized by court order;
  - o To auditors and evaluators;
  - o To researchers if the information will be protected as required by Federal regulations;
  - o To report suspected child abuse or neglect; and
  - o To report a crime or a threat to commit a crime on program premises or against program personnel.
- A statement that other disclosures will be made only with the patient’s written consent or authorization which can be revoked, unless the program has taken action in reliance on the consent or authorization. ;[20]
- A statement that the program may contact the patient to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the patient;[21]
- A statement that it is required by law to maintain the privacy of PHI and to notify patients of its legal duties and privacy practices, including any changes to its policies;
- A statement that the program must abide by the terms of the notice currently in effect; a statement that the program reserves the right to change the terms of its notice and to make the new notice provisions effective for all information it maintains;[22] and a statement describing how it will provide patients with a revised notice of its practices;

[19] The Privacy Rule also requires that the notice contain information about any more restrictive law. For example, if State law further limits disclosure of HIV-related information, that restriction should also appear in the notice.[20]

Programs often need to provide PHI to criminal justice agencies that mandate patients into treatment. Under Part 2, such disclosures may be made pursuant to a non-revocable consent that complies with 42 CFR §2.35. Under the Privacy Rule, such disclosures may be made pursuant to an authorization or pursuant to a court order. In order to comply with both rules, programs may find it helpful to ask the court in such a situation to issue an order that the program disclose necessary information to the court and other law enforcement personnel.[21] A substance abuse treatment program engaging in these kinds of activities must be careful in contacting the patient that it does not make any patient-identifying disclosures to others. If the program does not intend to contact the patient, they do not need to include this statement.[22] This is also voluntary. However, if this statement is not included, any changes in privacy practices described in the notice will apply only to PHI the program created or received after issuing a revised notice reflecting such changes. 45 CFR §164.520(b)(1)(v)(C).

- The name or title and telephone number of a person or office the patient can contact for further information;
- • A statement of the patient's rights with respect to PHI and a brief description of how the patient may exercise those rights, including:
  - o The right to request restrictions on certain uses and disclosures of PHI, including the statement that the program is not required to agree with requested restrictions;
  - o The right to receive confidential communications of PHI (such as having mail and telephone calls be limited to home or office location);
  - o The right to access and amend PHI;
  - o The right to receive an accounting of the program's disclosures of PHI;
  - o The right to complain—free from retaliation—to the program and to the Secretary of Health and Human Services (HHS) about violations of privacy rights, and information on how to file a complaint with the program; and
  - o The right to obtain a paper copy of the notice upon request.
- The effective date of the notice.

See 45 CFR §164.520(b).

2. Distribution of the Notice

Part 2 requires that programs provide the notice at the time of admission or as soon thereafter as the patient is capable of rational communication. See 42 CFR §2.22(a). The Privacy Rule requires that the substance abuse treatment program must provide the notice to a patient on the date of the first service delivery, including service delivered electronically, after April 14, 2003.[23] The program must also have the notice available on site for patients to request to take with them and posted in a clear and prominent location where it is reasonable to expect patients to be able to read it. Whenever there is a material change to the notice, the notice must be promptly revised, made available upon request, and re-posted as previously referenced. See 45 CFR §§164.520(c)(2); 164.530(i)(4)(i)(C).

The program must make a good faith effort to obtain patients' written acknowledgment of receipt of the notice, except in an emergency treatment situation, on the date of the first service delivery. If written acknowledgment is not obtained, the program must document its efforts and the reason it was not able to obtain the acknowledgement. See 45 CFR §164.520(c)(2)(ii).

Any program that maintains a web site that provides information about its services or benefits must prominently post its notice on the site and make it available electronically through the site. When patients agree, the program can provide the notice by e-mail. See 45 CFR §164.520(c)(3).

[23] There is an exception in emergency situations. If treatment is provided on an emergency basis, the program must provide the notice as soon as practicable after the emergency is resolved. See 45 CFR §164.520(c)(2)(i)(B).

B. Patient rights

The Privacy Rule provides patients with new Federal privacy rights, including the right to request restrictions of uses and disclosures of PHI, and the right to access, amend, and receive an accounting of disclosures of PHI. See 45 CFR §§164.522, 164.524, 164.526,164.528.

1. Right to request a restriction of uses and disclosures

The Privacy Rule requires that programs allow patients to request that the program restrict uses or disclosures of PHI for the purpose of treatment, payment or health care operations and for involvement in the patient's care and notification under 45 CFR §164.510(b). The program is not required to agree to a requested restriction. If, however, a program agrees to a restriction, the program may not then violate the agreed-upon restriction, except for emergency treatment purposes, so long as the program requests that the emergency treatment provider not further use or disclose the PHI. A covered entity may terminate the agreement to a restriction, effective after the patient has been informed of the termination. See 45 CFR §164.522(a).

The Privacy Rule gives the individual the right to request that communication of PHI be done by alternative means or to alternative locations (confidential communications). See 45 CFR §164.522(b)(1)(i). This might include the right to request that mail and telephone calls be limited to home or office location. The Privacy Rule requires programs to accommodate reasonable requests.

2. Right to access PHI

Neither Part 2 nor the Privacy Rule requires programs to obtain written consent from individuals before permitting them to see their own records. Likewise, neither rule prohibits a program from giving a patient access to his or her own records, including the opportunity to inspect and copy any records that the program maintains about the patient. 42 CFR §2.23. However, the Privacy Rule permits programs to require that such requests be in writing. See 45 CFR §164.524(b)(1). The Privacy Rule provides patients with a right of access to inspect and obtain a copy of their PHI. See 45 CFR §164.524(a)(1).[24] Certain information, however, is exempt from this right of access:

[24] The Privacy Rule requires access to information in a designated record set for as long as the PHI is maintained in the designated record set. "Designated record set" is defined as "[a] group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals." 45 CFR §164.501. The program must document the designated record sets that are subject to access and the titles of the persons or offices responsible for receiving and processing requests for access (45 CFR §164.524(e)). It must retain the documentation for six (6) years from the date it was last effective, whichever is later (45 CFR §164.530(j)). Under Part 2, the information need not be contained in a designated record set. Thus, programs could permit access to all disclosable patient records.

- Psychotherapy notes;[25]
- Information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding; and
- Information that may be subject to or exempt from certain Clinical Laboratory Improvement Amendment (CLIA) provisions.

See 45 CFR §164.524(a)(1).

The Privacy Rule requires that programs respond to a patient's request for access within 30 days after receipt of the request (within 60 days if the information is not maintained or accessible on-site). The program may extend the deadline once by not more than 30 days, if within 30 days of the receipt of the request (or 60 days of receipt if the information is not on-site), the patient is provided with a written statement containing the reasons for the delay and the date by which it will permit access. See 45 CFR §164.524(b). If the program does not maintain the requested information, but knows where the requested information is maintained, it must inform the patient where to direct his or her request. See 45 CFR §164.524(d)(3).

If a program grants the patient's request for access to his or her records, it can charge the patient a reasonable, cost-based fee, consistent with the restrictions on fees as provided in the Privacy Rule. See 45 CFR §164.524(c)(4).[26]

Denial of Access

The Privacy Rule allows a program to deny a patient access without providing an opportunity for review of the denial, on the following grounds:

- The information is specifically exempted from the right of access by the Privacy Rule. See 45 CFR §164.524(a)(1);
- The program is a correctional institution or a provider acting under the direction of the correctional institution and denies in whole or in part an inmate's request to obtain a copy of his or her records if doing so would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of an officer, employee or other person at the correctional institution or responsible for transporting the inmate. See §164.524(a)(2)(ii));
- The requested information was created or obtained by a program in the course of research that includes treatment.

[25] The Privacy Rule defines "psychotherapy notes" 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 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, the treatment plan, symptoms, prognosis, and progress to date." 45 CFR §164.501. [26] Information obtained by patient access to his or her own record is subject to Part 2's restriction on use of the information to initiate or substantiate any criminal charges against the patient or to conduct any criminal investigation of the patient. See 42 CFR §2.23(b). may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research and the program has informed him or her that the right of access will be reinstated upon completion of the research. See 45 CFR §164.524(a)(2)(iii);

- The requested information is subject to the Privacy Act and would be denied under the access provisions of the Privacy Act, 5 USC §522a. See 45 CFR §164.524(a)(2)(iv); or
- The requested information was obtained under a promise of confidentiality from someone other than a health care provider and such access would be likely to reveal the source of the information. See 45 CFR §164.524(a)(2)(v).

The Privacy Rule permits a program to deny patient access, provided that the patient is given the right to have such a denial reviewed, on the following grounds:

- 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 patient or another person;
- The information makes reference to another person (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access is reasonably likely to cause substantial harm to such other person; or
- The request for access is made by the patient's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

See 45 CFR §164.524(a)(3).

If the program's denial is based on one of the last three reasons, the patient has the right to have that denial reviewed by a licensed health care professional who is designated by the program to act as a

reviewing official and who did not participate in the original decision to deny access. See 45 CFR §164.524(a)(4).

If the program denies a patient access to all or parts of his or her PHI, it must give the patient a timely denial written in plain language containing:

- The basis for the denial;
- If applicable, a statement of the patient's review rights, including a description of how the patient may exercise those rights; and
- A description of how the patient may complain to the program or to the Secretary of HHS. The description must include information regarding how the patient may complain to the program pursuant to the program's complaint procedures or to the Secretary, and must include the name or title, and telephone number of the contact person or office designated by the program to receive complaints.

See 45 CFR §164.524(d)(2).

A program that denies a patient access in part must give the patient access to any other PHI requested after excluding the information to which the program had reason to deny access. See 45 CFR §164.524(d)(1).

3. The right to amend PHI

The Privacy Rule gives patients the right to have the program amend their PHI or a record about the patient in a designated record set. See 45 CFR §164.526. The program must act on a patient's request for amendment within 60 days after it receives the request. The program may extend the deadline once by not more than 30 days if, within the 60 days, the patient is provided with a written statement of the reasons for the delay and the date by which it will respond. See 45 CFR §164.526(b)(2).

A program that accepts a patient's request to amend PHI must:

- Timely inform the patient of its decision to accept the amendment;
- Make the appropriate amendment by 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
- • If the patient agrees, make reasonable efforts to notify and provide the amendment within a reasonable period of time to:
    - o Persons identified by the patient as having received the patient's PHI and needing the amendment; and
    - o Persons, including business associates, that the program knows to have received 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 patient.

See 45 CFR §164.526(c).

A program must obtain patient consent on forms that comply with 42 CFR §2.31 before it provides any copies of the amendment to other persons or organizations.

Denial of Amendment

A program may deny a patient's request for amendment if it determines that:

- It did not create the information, unless the patient provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
- The information or record is accurate and complete

The information that is the subject of the request is not part of a designated record set or would not otherwise be available for inspection under the Privacy Rule's request for access provisions.

See 45 CFR §164.526(a)(2).

If a program denies a patient's request to amend records, it must give him or her a timely denial, written in plain language, and contain:

- The basis for the denial;
- Notice of the patient's right to file a written statement of disagreement with the denial and how the patient may file such a statement;
- Notice that, if the patient does not submit a statement of disagreement, the patient may request that the program include his or her request for amendment and its denial with any future disclosures of the PHI that is subject to the amendment; and
- A description of how the patient may complain about the program's actions to the program or to the Secretary of HHS. The description must include information regarding how the individual may complain to the program pursuant to its complaint procedures or to the Secretary, and must include the name or title, and telephone number of the contact person or office designated by the program to receive complaints.

See 45 CFR §164.526(d)(1).

The program may prepare a written rebuttal to the patient's statement of disagreement. If it prepares such a rebuttal, it must provide a copy to the patient who submitted the statement of disagreement. This information (e.g. the statement of disagreement and rebuttal), or in some cases, a summary, must all be included in any subsequent disclosures of the information to which the disagreement relates as provided in 45 CFR §164.526(d)(3), (4), and (5).

The program must document the titles of the persons or offices responsible for receiving and processing requests for amendment. It must retain the documentation for six (6) years from the date it was created or last effective, whichever is later. See 45 CFR §164.526(f).

4. Right to an accounting of disclosures of PHI

The Privacy Rule provides individuals with the right to obtain an accounting of certain disclosures of PHI made by a program during the six (6) years prior to the request. See 45 CFR §164.528(a).

A program does not have to provide an accounting for any disclosures that were made:

- For treatment, payment, and health care operations as provided in 45 CFR §164.506;
- To the patient as provided in 45 CFR §164.502;
- Incident to a use or disclosure that is otherwise permitted as provided in 45 CFR §164.502;
- Pursuant to the patient's written consent (an "authorization" meeting the Privacy Rule's requirements at 45 CFR §164.508);
- For the facility's directory or to persons involved in the patient's care or other notification purposes as set forth by the rule at 45 CFR §164.510;
- For national security or intelligence purposes as provided by the rule at 45 CFR §164.512(k)(2);
- To correctional institutions or law enforcement officials having custody of an inmate or individual and as specified under 45 CFR §164.512(k)(5);
- As part of a limited data set in accordance with the rule at 45 CFR §164.514(e); and
- Before April 14, 2003.

See 45 CFR §164.528(a)(1). In addition, a program must temporarily suspend a patient's right to receive an accounting of disclosures to a health oversight agency or law enforcement official if the program receives notification that it would be reasonably likely to impede the activities of the agency or official. See 45 CFR §164.528(a)(2).

The accounting must be in writing[27] and include:

- The date of each disclosure;
- The name and address (if known) of the entity or person who received the PHI;
- A brief description of the PHI disclosed; and
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of a written request for disclosure, if any.

See 45 CFR §164.528(b)(2).

For substance abuse treatment programs, the following disclosures are typically made without patient consent and must therefore be included in an accounting of disclosures:

- Disclosures to health oversight agencies;
- Disclosures to researchers that include patient-identifying information;[28]
- Disclosures to public health authorities;[29]

[27] There are special provisions under the Privacy Rule that are applicable to accounting for recurrent disclosures and certain research disclosures. See 45 CFR §§164.528(b)(3) and (b)(4). [28] There are special provisions under the Privacy Rule that are applicable to accounting for research. See 45 CFR §164.528(b)(4)).

- Court-ordered disclosures;
- Reports of patient crimes on program premises or against program personnel; and
- Child abuse and neglect reports.

Programs should establish mechanisms to document all disclosures for which they must account.

The accounting must be made within 60 days of the program's receipt of the request. The program may extend the deadline once by not more than 30 days if, within the 60 days, the patient is provided with a written statement of the reasons for the delay and the date by which it will provide the accounting. A program must respond to a patient's request for one accounting within any 12-month period without charge. For any subsequent request within a 12-month period, it may charge a patient a reasonable, cost-based fee. If the program imposes a fee, it must inform the patient of the fee in advance and give the patient an opportunity to withdraw or modify the request. See 45 CFR §164.528(c).

The program must also document the following:

- The information it was required to provide the patient;
- The written accounting it provided the patient; and
- The titles of the persons or offices responsible for receiving and processing requests for an accounting.

This documentation must be retained for six (6) years from the date created or last effective, which ever is later. See 45 CFR §164.528(d).

C. Administrative Requirements

1. Complaints about the program's privacy practices

Part 2 allows violations of those regulations to be reported to the United States Attorney for the judicial district in which the violation occurs. See 42 CFR §2.5.

The Privacy Rule establishes a process for individuals to file a complaint with the Secretary of HHS if they believe a program violated the Privacy Rule. The complaint must be written, either on paper or electronically, and filed with HHS' Office for Civil Rights within 180 days of when the complainant knew, or should have known, that the act or omission complained of occurred, unless a waiver is granted. The complaint must name the program and describe the violation of the Privacy Rule. See 45 CFR §160.306. Programs must also establish a process for individuals to make complaints about the program's privacy policies and procedures.

2. Other administrative requirements

Programs subject to the Privacy Rule are required to meet administrative requirements including:

- Designate a privacy official who is responsible for the development and implementation of its policies and procedures and a contact person or office responsible for receiving complaints and able to provide further information. See 45 CFR §164.530(a).
- Train all members of the workforce on the program's policies and procedures. Each new member of the workforce must receive training within a reasonable period of time after s/he joins the workforce. Whenever a workforce member's functions are affected by a material change in privacy policies or procedures, that person must receive additional training within a reasonable period of time after the material change becomes effective. The program must document all training and retain the records for a period of six (6) years after the training. See 45 CFR §164.530(b).
- Have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. See 45 CFR §164.530(c).
- Establish written policies and procedures that identify the staff persons or classes of persons who need access to patients' PHI, the categories of PHI they need access to, and any conditions appropriate to such access. The program must make reasonable efforts to limit access based on these determinations. See 45 CFR §164.514(d)(2).
- Establish policies and procedures to ensure that, for disclosures of information that occur on a routine and recurring basis, reasonable efforts are made to limit disclosures to the minimum necessary to accomplish the intended purpose of the disclosure. See 45 CFR §§164.502(b) and 164.514(d)(3)(i). For "all other disclosures," the program must develop criteria designed to limit the information it discloses to the information reasonably necessary to accomplish the purpose for which disclosure is sought and review requests for disclosure on an individual basis in accordance with those criteria. See 45 CFR §164.514(d)(3)(ii). Programs must also develop policies, procedures and criteria to ensure that requests to

other entities subject to the Privacy Rule for PHI are limited to information "which is reasonably necessary to accomplish the purpose for which the request is made." See 45 CFR §164.514(d)(4). The written polices and procedures must be retained for six (6) years after the last time they were effective. See 45 CFR §164.530(j).

- Establish and apply appropriate sanctions against members of its workforce who fail to comply with its privacy policies and procedures. See 45 CFR §164.530(e)

- Mitigate, to the extent practicable, any harmful effect that is known to the program that results from a use or disclosure in violation of its policies and procedures. See 45 CFR §164.530(f).
- Refrain from taking intimidating, threatening, coercing, discriminating, or other retaliatory action against any individual who exercises rights under the Privacy Rule, including filing a complaint, assisting in an investigation, compliance review, proceeding or hearing pursuant to the Privacy Rule, as well as any individual who opposes any act or practice made unlawful by the Privacy Rule, provided that he or she has a good faith belief that the practice is unlawful and the manner of opposition is reasonable and does not invoke an impermissible disclosure of PHI. See 45 CFR §164.530(g).
- Not require patients to waive their rights to complain to the Secretary of HHS or their other rights under the Privacy Rule as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits. See 45 CFR §164.530(h).
- Implement policies and procedures regarding PHI that are designed to comply with the standards, implementation specifications, and other requirements of the Privacy Rule, and maintain the policies and procedures in written or electronic form for six years from the date the document was created, or last effective, whichever is later. See 45 CFR §164.530(i) and (j).

D. Security of information

Part 2 requires programs to maintain patient written records in a secure room, locked file cabinet, safe or other similar container. The regulations also require programs to adopt written procedures to regulate access to patients' records. See 42 CFR §2.16.

Section 164.530(c) of the Privacy Rule requires programs to maintain reasonable and appropriate administrative, technical and physical safeguards to protect the privacy of PHI. The issue of security has been addressed in more detail through a separate Security Rule issued by HHS on February 20, 2003 that established the physical and technical security standards required to guard the integrity, confidentiality and availability of confidential information that is electronically stored, maintained or transmitted. See 68 Federal Register 8334. Covered entities must be in compliance with the Security Rule by April 20, 2005, except small health plans which have until April 20, 2006.

Conclusion

Compliance with Part 2 has given the substance abuse treatment programs extensive experience with protecting patient confidentiality. Although substance abuse programs will need to make some changes to their business practices, they have a good starting point to work from in achieving compliance with the HIPAA Privacy Rule. Substance abuse treatment programs should contact their respective State substance abuse agencies and/or provider organizations, as well as legal counsel for assistance in implementing practices that will comply with both Part 2 and the Privacy Rule.

For more information about the HIPAA Standards

http://www.hipaa.samhsa.gov is the SAMHSA website which provides information and links for all HIPAA standards.

Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 and 164) More information can be obtained from the Office for Civil Rights HIPAA website

http://hhs.gov/ocr/hipaa

Standards for Electronic Transactions (45 CFR Parts 160 and 162) The Standards for Electronic Transactions can be obtained from the Center for Medicare and Medicaid Services (CMS) website at

http://cms.gov/hipaa/hipaa2/default.asp

Standard Unique Employer Identifier (45 CFR Parts 160 and 162)

http://cms.gov/hipaa/hipaa2/default.asp

Security Standards (45 CFR Parts 160, 162 and 164)

http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

http://www.hhs.gov/ocr/hipaa

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES Substance Abuse and Mental Health Services Administration Center for Substance Abuse Treatment www.samhsa.gov