DEPARTMENT OF HEALTH & HUMAN SERVICES Health Resources and Services Administration

HIV/AIDS Bureau

Rockville, Maryland 20857

April 2004

Dear Colleague:

The Health Insurance Portability and Accountability Act (HIPAA), enacted on August 21, 1996, impacts all areas of the health care industry. HIPAA was designed to provide insurance portability, improve the efficiency of health care by standardizing the exchange of administrative and financial data, and protect the privacy, confidentiality and security of health care information. The Health Resources and Services Administration (HRSA) and the HIV/AIDS Bureau (HAB) recognize the importance of these provisions for its grantees and service providers by publishing the enclosed resource guide entitled "Protecting Health Information Privacy and Complying with Federal Regulations".

One part of HIPAA establishes new Federal Standards for Privacy of Individually Identifiable Health Information (hereafter, referred to as the Privacy Rule), which requires compliance by health care providers to assure patient confidentiality and other patient rights are in place. In April 2003, most entities subject to the new Privacy Rule were required to be compliant with the rule. The Privacy Rule establishes new responsibilities and requirements for certain individuals and organizations when they use or disclose certain individually identifiable health information.

HRSA and HAB developed the enclosed resource guide to assist Ryan White Comprehensive AIDS Resources Emergency (CARE) Act grantees, who are defined as "covered entities" under HIPAA, to comply with the Privacy Rule. This guide has attempted to highlight provisions of the Privacy Rule that are especially relevant to CARE Act grantees.

Some provisions of the Privacy Rule may be omitted. Reading this guide should not substitute for reading the full text of the Privacy Rule. Grantees are encouraged to obtain and read the complete text of the Privacy Rule. Although this resource guide may be helpful in the implementation of the HIPAA Privacy Rule in your facility, it should not be considered legal advice. In assessing your responsibilities under the Privacy Rule, it may be necessary for you to consult with legal counsel as you take steps for compliance.

We hope that this document is able to provide some level of assistance to you, your sub-grantees and contractors with the HIPAA Privacy Rule. If you have questions about this letter, please contact your HAB Project Officer. Should you require additional information about HIPAA, you can access HRSA's HIPAA web site at: http://www.hrsa.gov/hipaa.htm, or for specific information about the Privacy Rule, you should access the Office for Civil Rights web site at: www.hhs.gov/ocr/hipaa/.

Sincerely,

Deborah Parham Hopson

Deborah Parham Hopson, Ph.D., R.N.
RADM, USPHS
Associate Administrator

Enclosure

Protecting Health Information Privacy and Complying with Federal Regulations

A Resource Guide for HIV Services Providers and the Health Resources and Services Administration's HIV/AIDS Bureau Staff

April 2004

U.S. Department of Health and Human Services
HRSA
Health Resources and Services Administration

Table of Contents

Prepared by Health Resources and Services Administration staff, in consultation with the Office of the General Counsel, the Office for Civil Rights, other offices and agencies within the U.S. Department of Health and Human Services, Washington, D.C., and health privacy specialists.

This resource guide is provided for Ryan White Comprehensive AIDS Resources Emergency (CARE) Act grantees and program staff in the Health Resources and Services Administration's (HRSA) HIV/AIDS Bureau (HAB) to help in understanding key aspects of the medical Privacy Rule and to assist covered individuals or organizations in complying with the Privacy Rule.

Introduction

On April 14, 2003, most entities subject to the new Federal Standards for Privacy of Individually Identifiable Health Information (hereafter, the Privacy Rule) were required to be compliant with the rule. The Privacy Rule establishes new responsibilities and requirements for certain individuals and organizations when they use or disclose certain individually identifiable health information.[1] The Privacy Rule was adopted as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and provides individuals with new rights related to their own health information.[2] HIPAA is a law that established Federal requirements governing the group health insurance market—including limiting the ability of health insurers to deny coverage based on pre-existing condition exclusions. It also established a guaranteed right of access to individual insurance coverage for certain persons who lose access to group coverage.

Another aspect of HIPAA is a group of provisions, collectively referred to as Administrative Simplification. These provisions are intended to improve the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the adoption of standards for electronic transmission of certain health information. HIPAA provides for the establishment of uniform standards for claims and other financial and administrative transactions and requires the adoption of new privacy and security standards for the handling of certain individually identifiable health information. The Privacy Rule is a critical part of Administrative Simplification. The Department of Health and Human Services (HHS) has issued or is developing a series of regulations to implement the various Administrative Simplification provisions of HIPAA; the Privacy Rule is just one part of this effort.

The Privacy Rule became enforceable against health care providers that are covered by the HIPAA Privacy Rule, many health plans, and health care clearinghouses on April 14, 2003. Small health plans (those with annual receipts of $5 million or less) have an additional year, until April 14, 2004, to comply. 45 CFR §164.534. Collectively, these entities (health plans, health care clearinghouses, and covered health care providers) are known as **covered entities.** 45 CFR §160.103.

This guide has attempted to highlight provisions of the Privacy Rule that are especially relevant to Ryan White CARE Act grantees. Therefore, some provisions of the Privacy Rule may be omitted. Reading this guide **should not** substitute for reading the full text of the Privacy Rule. HAB and its grantees are encouraged to obtain and read the complete text of the Privacy Rule.

[1] 45 CFR Parts 160 and 164, Subparts A and E.
[2] Public Law 104-191, also called the Kassebaum/Kennedy law.

This resource guide should not be considered legal advice. In assessing their responsibilities under the Privacy Rule, it may be necessary for covered entities to consult with legal counsel as they take steps to comply with the Privacy Rule.

A compilation of the provisions of the HIPAA Privacy Rule (as updated through April 2003), HHS guidance, and other resources are available from the HHS Office for Civil Rights (OCR), the agency that is responsible for the implementation and civil enforcement of the Privacy Rule. This information is available at:

www.hhs.gov/ocr/hipaa/

For historical information and additional background information, as well as information about other Administrative Simplification issues, the HHS Assistant Secretary for Planning and Evaluation (ASPE) maintains a HIPAA Administrative Simplification website. This site can be found at:

http://aspe.hhs.gov/admnsimp/index.shtml

The HHS Centers for Medicare and Medicaid Services (CMS) has responsibility for implementing and enforcing the remaining HIPAA Administrative Simplification regulations, including the security and transaction standards regulations. Additional HIPAA Administrative Simplification information from CMS is available at:

www.cms.gov/hipaa/hipaa2

KEY ISSUES ADDRESSED IN THE RESOURCE GUIDE

The guide describes the major provisions of the Privacy Rule and is organized around answering nine fundamental questions:

1. Who is covered by the Privacy Rule?
2. What information is covered by the Privacy Rule?
3. What rights do individuals have with regard to their own health information?
4. What does the Privacy Rule require regarding uses and disclosures of protected health information?
5. What disclosures are permitted without individual authorization?
6. How much information can be used and disclosed?
7. What is the impact of the Privacy Rule on information sharing with, or reporting to the HRSA HIV/AIDS Bureau (HAB)?
8. What steps must covered entities take to comply with the Privacy Rule?
9. How is the Privacy Rule enforced?

****

1. Who is covered by the Privacy Rule?

The Privacy Rule applies to all health plans and health care clearinghouses. It also applies to health care providers who transmit health information in electronic form in connection with specified financial and administrative transactions (such as claims for payment). Individuals and organizations that must comply with the Privacy Rule are collectively referred to as **covered entities**. 45 CFR §160.103.

- A health plan generally includes any individual or group plan that provides or pays for medical care. The term encompasses both private and governmental plans. HMOs and certain high-risk pools are specifically covered. Most employee health benefit plans are covered. However, *employers* who sponsor group health plans are *not* covered entities under the Privacy Rule. [Government-funded programs whose principal purpose is other than providing or paying the cost of health care are not health plans.] Government-funded programs that have as their principal activity the direct provision of health care, the making of grants for the direct provision of health care, or the funding of the direct provision of heath care are also not health plans, but they may meet the definition of a health care provider.

    - **Ryan White CARE Act grantees are generally not health plans (unless they receive funding from another source and meet the definition of a health plan). Ryan White CARE Act grantees may be covered health care providers.**

- Under the Privacy Rule, a health care clearinghouse is an entity that translates health information received from other entities either to or from the standard format that is required for certain electronic transactions. For instance, a health care provider may submit claims information to a health care clearinghouse to process that information into a standard format for submission to a health plan.

- The Privacy Rule also covers health care providers who transmit health information in electronic form in connection with transactions for which the Secretary has adopted standards.

  Health care providers are covered entities if they meet a three-prong test (see next page). Further, some individuals and organizations may be covered health care providers who do not think of themselves as being health care providers. The definitions of health care and health care providers in the Privacy Rule are broad. For example, case managers may be covered health care providers even if they do not provide direct medical care.

Many Ryan White CARE Act grantees, for example, provide health care services and submit electronic claims to Medicaid. Doing this makes an organization a covered entity.

3- PART TEST FOR COVERED HEALTH CARE PROVIDERS

To determine whether a health care provider is covered by the Privacy Rule, answer the following questions:

1. Is the person or organization considered a *health care provider*?

   A health care provider is any person or organization that furnishes, bills, or is paid for health care in the normal course of business. Health care is broadly defined by the Privacy Rule to include preventive, diagnostic, therapeutic, and rehabilitative counseling services, assessments, and procedures with respect to the physical or mental condition or functional status of an individual. It also includes the sale or dispensing of drugs, devices, and equipment with a prescription. Thus, the term *health care provider*, includes both persons (such as dentists and podiatrists) and facilities (such as hospitals and clinics). It includes mainstream practitioners (such as physicians, nurses, and psychotherapists), as well as providers of alternative care (such as homeopaths, acupuncturists, and naturopaths). The term **health care provider** covers both the providers of care and services (such as practitioners) and the providers of health supplies (such as pharmacists and hearing aid dispensers).

2. Does the person or organization conduct covered transactions?

   To come within the scope of the Privacy Rule, the health care provider must transmit health information in connection with any of the transactions for which the Secretary of HHS has adopted a standard. As of the date of this Guide, these include:

   (A) Health claims or equivalent encounter information;
   (B) Enrollment and disenrollment in a health plan;
   (C) Eligibility for a health plan;
   (D) Health care payment and remittance advice;
   (E) Health plan premium payments;
   (F) Health claim status;
   (G) Referral certification and authorization; and
   (H) Coordination of benefits.

   AND

3. Does the person or organization transmit health information in electronic form in connection with any of these transactions?

   Does the person or organization conduct any of the listed transactions using electronic storage or transmission media (see 45 CFR §160.103 for the definition of electronic media)? This would include, but not be limited to, the Internet, an Intranet, a private network system, or transfer or storage using magnetic tape or disk. Does the person or organization have someone else transmit information electronically on its behalf? Any of these will bring the provider within the Privacy Rule. If, however, the provider and its business associates only transmit health information in connection with the covered transactions listed above via paper facsimile or by voice via telephone, the provider would not be covered because the provider would not have transmitted any health information in electronic form in connection with a covered transaction.

If the answers to Questions 1, 2 and 3 are all YES, then the provider is a covered entity.

RECOMMENDED ACTIONS

1) Obtain a copy of the final version of the Privacy Rule. You can download a free copy from the Office for Civil Rights at www.hhs.gov/ocr/combinedregtext.pdf.

2) Determine if you or your organization is a covered entity. To make this determination, view the online "Covered Entity Decision Tools" on the Office for Civil Rights website: www.hhs.gov/ocr/hipaa or the Centers for Medicare and Medicaid Services (CMS) website: www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp

3) Appoint an individual to take lead responsibility for assuring compliance with the Privacy Rule.

4) Seek out free online and other resources to become as fully informed as possible. HHS' Office for Civil Rights has a number of resources available at www.hhs.gov/ocr/hipaa. Covered entities whose operations are complex or that raise complicated legal questions regarding how to comply may wish to consider hiring a lawyer or consultant to help them assess their responsibilities under the Privacy Rule.

2. What information is covered by the Privacy Rule?

Generally, the Privacy Rule covers **protected health information** in any form that is transmitted or maintained by a covered entity (i.e. oral, written, and electronic information). 45 CFR §160.103.

The Privacy Rule protects the health information of both living and deceased individuals. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g, are expressly excluded, as are employment records.

- **Once an organization or person becomes a covered entity, individually identifiable health information that is created, maintained, or received by the covered entity is covered by the Privacy Rule (with certain exceptions, as noted above) — including paper records.**

- **In most cases, covered entities cannot segregate information by payer and comply with the Privacy Rule for Medicaid clients, for example, and not comply with the Privacy Rule for CARE Act-funded clients.**

WHAT IS PROTECTED HEALTH INFORMATION?

Protected health information is individually identifiable health information transmitted or maintained in any form or medium (including oral communications, paper records, and electronic records) by covered entities or their business associates. Education records and employment records are not protected health information.

Key components of the *protected health information* definition [45 CFR §160.103] are:

1. Health information

   Health information is broadly defined as any oral or recorded information relating to the past, present or future physical or mental health of an individual, the provision of health care to the individual, or the payment for health care. This definition is broad enough to encompass not only the traditional medical record but also physicians' personal notes and billing information.

2. Individually identifiable

   Individually identifiable health information is health information that identifies or can be used, alone or in combination with other information, to identify the individual. Health information that has been *de-identified* is not covered by the Privacy Rule. A covered entity may de-identify health information by removing specific identifiers. To be considered de-identified, at least 18 identifiers must be removed, such as name, social security number, medical record number, and address. Further, the covered entity must have no actual knowledge that the remaining information could be used to identify the individual. Alternatively, a covered entity may treat information as de-identified if a qualified statistician, using generally accepted statistical and scientific principles, determines that the risk is very small that the individual could be identified.

3. Created or received by a covered entity.

   Most individually identified health information that is created or received by, or on behalf of, a covered entity is protected under the Privacy Rule. In contrast, health information that is created or received by others who are not business associates of the covered entity is not covered. For example, if an individual fills out a health assessment survey as part of donating blood to a blood bank, that information would not be protected by the Privacy Rule if the blood bank is not a covered entity or the business associate of a covered entity.

RECOMMENDED ACTIONS

1) Carefully read the definition of health information in the Privacy Rule.

2) Do an assessment of all information collected and maintained by you or your organization. This includes any information your clients provide to you, even if you may not think it is related to health, including contact information, billing, and insurance information.

3) Carefully read the Privacy Rule provisions regarding de-identifying information. Certain information, such as aggregate information about all of your clients, may not be individually identifiable. This information is not protected health information. Care is needed…information that has no name or social security number often is individually identifiable if it still can be used alone or in combination with other information to identify an individual who is its subject.

3. What rights do individuals have with regard to their own health information?

The Privacy Rule gives individuals the right to control the use and disclosure of their own health information, except as otherwise specifically permitted or required by the Privacy Rule. The Privacy Rule also establishes new rights for individuals with respect to their protected health information, including the right of access to their protected health information, the right to request amendment of their protected health information (such as when they believe the record contains incorrect information), the right to receive notice of a covered entity's privacy practices, the right to request privacy protection for their protected health information, and the right to receive an accounting of certain disclosures. Each of these rights to the individual and the responsibilities of the covered entities are discussed in detail below.

For the most part, the rights afforded by the Privacy Rule are exercised by the *individual*, who is the person who is the subject of the protected health information.

In certain circumstances, however, a *personal representative* must be treated as the individual, and has the rights of the individual with respect to the individual's health information. 45 CFR §164.502(g). In general, the Privacy Rule provides that a person authorized under state or other law to act on behalf of the individual in making health care decisions is the individual's personal representative. Personal representatives can include parents, guardians, executors of estates, and others. The Privacy Rule provisions differ for personal representatives depending on whom they represent, reflecting the differing circumstances that arise in the context of various types of representation.

WHO EXERCISES PRIVACY RIGHTS? — SPECIAL CIRCUMSTANCES

Adults and emancipated minors

A person who is authorized by applicable law to act on behalf of an adult or emancipated minor in making decisions related to health care generally must be treated as the personal representative of that individual. This includes court-appointed guardians and persons with powers of attorney. The authority of a personal representative under this rule may be limited: the representative must be treated as the individual only to the extent that protected health information is relevant to the matters on which the personal representative is authorized to represent the individual. For example, a person who has a power of attorney with respect to an individual's lung cancer treatment probably would not have the authority to access the individual's mental health records. 45 CFR §164.502(g)(2).

Minors

Generally, a parent (or legal guardian or other person acting *in loco parentis)* is considered to be the personal representative of an unemancipated minor, and exercises the rights associated with the minor's health information (such as the right to authorize a disclosure or to request access to health information).

In certain circumstances, however, an unemancipated minor may exercise rights associated with his or her health information. The Privacy Rule gives a minor rights with respect to health information pertaining to a health care service where:

-- A minor authorized by law to consent to treatment has consented to care (with or without the consent of the parent);

-- A court or other legally authorized person consents to the care; or

-- A parent has assented to an agreement of confidentiality between a provider and a minor with respect to the care.

In these circumstances, the minor has the exclusive right to authorize the disclosure of the related health information (with the possible exception of disclosures to his or her parents). The minor also has the right of access to this health information.

The issue of disclosure to, and access by, parents of a minor's health information is more complicated, and is largely governed by state law. The Privacy Rule allows covered entities to disclose a minor's health information to a parent (or provide the parent with access to such information) if such disclosure (or access) is permitted or required by state law. Similarly, disclosure to (and access by) a parent is prohibited where prohibited by state law. Where state law is silent or unclear with respect to access by parents, the Privacy Rule permits a covered entity to provide or deny access to the parent so long as that action is consistent with state law *and* the decision is made by a licensed health care professional in the exercise of professional judgment.

State parental notification and consent to treatment laws are generally not affected by the Privacy Rule. 45 CFR §164.502(g)(3).

Victims of domestic violence, abuse, or neglect

Notwithstanding a conflict with state law or any of the provisions summarized in this block, a covered entity may elect not to disclose protected health information to a personal representative of an individual if the covered entity has a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by such person, and in certain other situations, and the covered entity decides that it is not in the individual's best interest to treat the person as the individual's personal representative. 45 CFR §164.502(g)(5).

Deceased Individuals

If under applicable law an executor, administrator, or other person has the authority to act on behalf of a deceased individual, that personal representative can exercise the rights of the individual with respect to relevant protected health information. 45 CFR §164.502(g)(4).

Right of access

The Privacy Rule establishes a new Federal right for individuals to see and obtain a copy of their protected health information in a designated record set for as long as the covered entity maintains the information. 45 CFR §164.524. It also establishes deadlines for covered entities to respond to requests for access and creates procedures for reviewing denials of those requests.

In general, the covered entity must allow the individual to inspect or obtain a copy of the protected health information in a designated record set in the form or format requested by the individual (if it is readily producible in such form or format) no later than 30 days after receiving the request and up to 60 days for information that is not on site. The deadline may be extended once up to an additional 30 days if the covered entity is unable to respond within 30 days provided the covered entity explains to the individual the reasons for the delay in writing. The covered entity can provide the individual with a summary of the requested protected health information, if the individual agrees in advance to the arrangement and the fees imposed, if any. The covered entity can impose reasonable, cost-based fees (not including costs of search and retrieval) for providing the individual a copy or summary of his or her protected health information. If the covered entity does not maintain the individual's protected health information, but knows where the requested information is kept, the entity must let the individual know where to direct his or her request for access.

DENYING INDIVIDUALS ACCESS TO THEIR OWN INFORMATION — SPECIAL CIRCUMSTANCES

A covered entity *may* deny an individual access to all or part of his or her protected health information in a designated record set *without* providing the individual an opportunity for review of that denial in the following circumstances [45 CFR §§164.524(a)(1) and (2)]:

-- Psychotherapy notes (psychotherapy notes are notes recorded in any medium by 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);

-- Information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding;

-- Protected health information maintained by a covered entity that is a laboratory that is either subject to Clinical Laboratory Improvements Amendments (CLIA) or exempt from CLIA regulations;

-- Information requested by an inmate from a correctional institution or a covered health care provider acting under the direction of the correctional institution, if providing a copy to the inmate would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates, or the safety of any officer, employee, or other person at the correctional institution or persons responsible for transporting of the inmate;

-- Research that includes treatment – access may be suspended until completion of the research, provided the individual had agreed to the denial of access when consenting to participate in the research, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research;

-- If the requested information is contained in records subject to the Privacy Act, and denial of access would meet the requirements of that Act; or

-- If the covered entity obtained the information from someone other than a health care provider under a promise of confidentiality and access would reasonably likely reveal the source of that information.

In the following three circumstances, a covered entity may deny an individual access to his or her protected health information, but it must provide an opportunity for review of that denial [45 CFR §164.524(a)(3)]:

-- A licensed health care professional, in the exercise of professional judgment, determines that it is reasonably likely that access to the requested information would endanger the life or physical safety of the individual or another person;

-- The requested information makes references to another person other than a health care provider and the licensed health care professional, in the exercise of professional judgment, determines that access is reasonably likely to cause substantial harm to that other person; or

-- The request for access is made by the individual's personal representative, and a licensed health care professional, in the exercise of professional judgment, determines that providing access to that representative is reasonably likely to cause substantial harm to the individual or another person.

If the covered entity denies an individual access to all or part of his or her protected health information, it must give the individual a written denial in plain language within 30 days or within 60 days if the protected health information is not accessible on-site. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, for which access is not being denied. The denial must contain the basis for the denial and, if applicable, a statement of the individual's review rights and a description of how the individual can exercise those rights. It also must include specific information on how the individual can file a complaint with the covered entity or with the Secretary of HHS.

If an individual requests a review of the denial, the covered entity must designate a licensed health care professional who was not directly involved in the initial decision to deny access to review the decision. The entity must promptly provide the individual written notice of the decision. 45 CFR §164.524(d).

Right to amendment of their protected health information

The Privacy 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. 45 CFR §164.526. For example, an individual who believes that information contained in his or

her record is incorrect can submit additional information to substantiate this claim. Individuals can also request that second opinions be included in their designated record set. The individual has the right to have a covered entity amend their protected health information for as long as the covered entity maintains the information in a designated record set. The covered entity must act on an individual's request for amendment no later than 60 days after it receives the request. The deadline may be extended once up to 30 days if the covered entity provides the individual with a written statement of the reasons for delay and the date by which the covered entity will fulfill his or her request. If a covered entity accepts the request it must: (1) make the appropriate amendment; and (2) inform the individual in a timely fashion that the amendment is accepted. The covered entity must then make reasonable efforts to provide the amendment within a reasonable time to both entities identified by the individual and other entities known to have received the erroneous information.

A covered entity may deny an individual's request for amendment if the entity determines that the information or record: (1) was not created by the covered entity unless the individual provides a reasonable basis to believe that the protected health information is no longer available to make the amendment; (2) is not a part of the designated record set; (3) would not be available for inspection; or (4) is accurate and complete. 45 CFR §164.526(a)(2).

If the covered entity denies an individual's request in whole or in part, it must give the individual a timely denial in plain language text, which includes the basis for the denial, the individual's right to submit a written statement disagreeing with the denial and how to exercise that right, a statement that the individual can request the covered entity to include the individual's request and the denial with any future disclosures of the information (if the individual does not file a statement of disagreement), and a description of how the individual can file a complaint with the covered entity or the Secretary of HHS. 45 CFR §164.526(d).

If the individual files a statement of disagreement, the covered entity can prepare a rebuttal to the individual's statement. The entity must provide a copy of the rebuttal to the individual. The request for amendment, the denial, the statement of disagreement (if submitted), and rebuttal (if any), or a summary of such information must be provided with any subsequent disclosures of the protected health information. The covered entity can set reasonable limits on the length of the individual's statement of disagreement.

Right to receive notice of a covered entity's privacy practices

The Privacy Rule requires covered entities to provide notice describing their privacy practices to the individual who is the subject of the protected health information. 45 CFR §164.520.

Health plans are required to give notice to named insureds by the compliance date of the Privacy Rule (April 14, 2003; small health plans – April 14, 2004) and to new named insureds at the time of enrollment. This means, for example, that for families receiving group health insurance coverage through an employer, only the employee, and not all family members, must be given notice. Health plans are also required to notify individuals every three years that the privacy practices notice is available. 45 CFR §164.520(c)(1).

Health care providers with direct treatment relationships with individuals are required to give notice of their privacy practices no later than the date of the first service delivery after April 14, 2003. Except in emergencies, health care providers with direct treatment relationships must also make a good-faith effort to obtain a written acknowledgment of receipt of the notice. All covered entities must make available the notice to any person, upon request. Health care providers with direct treatment relationships must post the notice on the premises if they maintain a physical service delivery site. 45 CFR §164.530(c)(2).

Covered entities also have special notice requirements if their privacy practices change. 45 CFR §§164.520(b)(1)(v)(C) and (b)(3).

- **Ryan White CARE Act grantees that are covered entities as health care providers must give written notice at least once — no later than the first date that services are provided after the compliance date. Notice must also be given upon request and when the provider's privacy policy changes. Providers must also post their notice of privacy practices on the premises of their facilities.**

NOTICE REQUIREMENTS

The notice must be written in plain language. HRSA has developed guidance for making privacy notices more readable. When developing a privacy notice, consult www.hrsa.gov/language.htm. The following are critical elements of the notice—other requirements also apply (covered entities should review 45 CFR §164.520 to ensure that they comply with all of the Privacy Rule's notice requirements):

-- The notice must contain as a header or prominently displayed the following statement: "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 of the individual's rights with respect to protected health information and how the individual may exercise those rights;

-- The legal duties of the covered entity;

-- A description of the types of uses and disclosures that are permitted with examples, including those permitted or required without the individual's written authorization;

-- How an individual can file complaints with the covered entity and a statement that the individual will not be retaliated against for filing a complaint;

-- A statement that individuals may complain to the Secretary of HHS if they believe their privacy rights have been violated;

-- A contact person for additional information; and

-- The date on which the notice is in effect.

It is important to note:

-- Separate statements are required in the notice for certain uses and disclosures. For example, if a covered entity plans to use or disclose protected health information for fundraising or to contact individuals to remind them of appointments, then they must specifically state in the notice that uses and disclosures may be made for these specific purposes.

-- The covered entity must expressly reserve its right to change the terms of its privacy notice and must specify that such changes will apply to previously created or received health information. If the entity does not reserve its rights to change a privacy practice stated in the notice, it is bound by the privacy practices in the notice with respect to protected health information created or received while that notice is in effect.

Right to request privacy protection of protected health information

The Privacy Rule gives individuals the right to request additional restrictions on uses and disclosures of their protected health information. This right to request additional restrictions and the right of a covered entity to deny that request are described in the next section following a description of general rules for uses and disclosures. 45 CFR §164.522.

Right to receive an accounting of disclosures

Individuals have the right to receive an accounting of disclosures of their protected health information made by the covered entity during the six years prior to the date (beginning on the compliance date) that the individual requests the accounting, including disclosures by business associates. 45 CFR §164.528. The right to an accounting only extends to *disclosures, i.e.*, sharing health information *outside* of a covered entity. It does *not* encompass *uses*, *i.e.*, sharing health information *within* a covered entity. For example, an individual does not have a right to a list of all hospital employees who have had access to his or her health information. With some exceptions, the accounting must include the date of each disclosure; the name and, if known, the address of the entity or person who received the information; a description of the information disclosed; and a brief statement of the purpose of the disclosure or a copy of the written request for disclosure. The Privacy Rule includes other accounting provisions for multiple disclosures of protected health information to the same person for certain purposes and for multiple disclosures for a particular research purpose. 45 CFR §§164.528(b)(3) and (4).

The covered entity must provide the individual with the accounting no later than 60 days after it receives the request. The deadline may be extended once up to 30 days. The first accounting provided to an individual in any 12-month period is free. The covered entity may impose a reasonable, cost-based fee for each subsequent request within the 12-month period. 45 CFR §164.528(c).

There are a few exceptions to the individual's right to receive an accounting of disclosures, and they are specified in the Privacy Rule. 45 CFR §164.528(a)(l)(i)-(ix). For example, the covered entity is not required to provide an accounting of disclosures that have been made to carry out treatment, payment, and health care operations. The Privacy Rule also exempts from the accounting requirement disclosures made pursuant to a valid authorization and disclosures that are part of a limited data set pursuant to a valid data use agreement. The covered entity must also temporarily suspend the individual's right to receive an accounting with respect to disclosures made to a health oversight agency or law enforcement official if the agency or

official provides the entity with a statement that providing the individual an accounting of the disclosure would reasonably likely impede agency activities. The statement must specify the suspension time required. 45 CFR §164.528(a)(2)(i).

REQUIRED ACTIONS

1) Develop policies and procedures for allowing clients to inspect and receive a copy of their own records. This includes establishing policies for charging a reasonable cost-based fee for copying records (if the covered entity elects to charge a fee).

2) Develop policies and procedures for allowing individuals to request amendments to their records and for acting on such requests, such as when an individual reports an error or disputes information contained in the record.

3) Develop policies and procedures for verifying which individuals can lawfully act as personal representatives.

4) Develop policies and procedures for when it may be necessary to deny access by individuals or their personal representatives to an individual's medical records.

5) Give notice of your privacy practices on the first service delivery date after the applicable compliance date. Consult www.hrsa.gov/language.htm for guidance on plain language and making the privacy notice more readable.

6) Post your notice of privacy practices on the premises (applies to covered entities with physical service delivery sites) and on your website.

7) Develop policies and procedures for evaluating and implementing requests from individuals for additional restrictions on uses and disclosures of their protected health information.

8) Train members of your workforce to understand and operationalize the requirements of the Privacy Rule.

9) Designate an individual as the privacy officer who is responsible for ensuring that privacy policies are followed.

4. What does the Privacy Rule require regarding uses and disclosures of protected health information?

The Privacy Rule establishes standards under which covered entities may use and disclose protected health information. They include required disclosures and permissive disclosures. As stated above, the Privacy Rule requires covered entities to disclose protected health information to individuals who are the subject of the protected health information when those individuals or their personal representatives request access, except in limited circumstances. The only other case in which the Privacy Rule requires covered entities to disclose information is to the Office for Civil Rights within the Department of Health and Human Services, when necessary to determine compliance with the Privacy Rule. All other uses and disclosures of protected health information are permissive. This means that the Privacy Rule allows covered entities to disclose

protected information, at their own discretion but, in many cases, subject to certain requirements or limitations. As discussed later, other laws or legal processes may compel covered entities to disclose protected health information. If a use or disclosure is not required or permitted by the Privacy Rule, a covered entity must obtain the individual's authorization for the intended use or disclosure.

Permissive uses and disclosures fall into four categories:

1) **Treatment, payment, and health care operations**

   Covered entities may use and disclose protected health information for treatment and payment without an individual's authorization. 45 CFR §164.502(a)(i)(ii). The Privacy Rule defines *treatment* as the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between providers relating to a patient; or the referral of a patient for health care from one health care provider to another. 45 CFR §164.501. *Payment* is defined as the activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan to an individual, or activities by a health care provider or health plan to obtain or provide reimbursement for the provision of health care to an individual. 45 CFR §164.501

   The Privacy Rule also permits uses and disclosures without authorization if they fall into a category of purposes called *health care operations*, a term intended to encompass the routine management functions of a well-run and efficient health care organization. Health care operations is a broad category that includes, but is not limited to: quality assessment and improvement activities; reviewing the competence or qualifications of health care professionals; arranging for legal services; business planning; training; customer services; resolution of internal grievances; underwriting; creating de-identified information; and certain fundraising activities. 45 CFR §164.501.

2) **Uses and disclosures for which individuals can agree or object**

   The Privacy Rule creates a category of uses and disclosures for which no authorization is required, but for which individuals must be given an opportunity to agree or object. Except in certain emergency conditions, individuals must be given an advance opportunity to agree or object to certain uses and disclosures by objecting to the use or disclosure. This applies to uses and disclosures related to facility directories (such as a list of patient names and room numbers available from a hospital information desk) and disclosures to certain persons related to, or identified by, the individual. 45 CFR §164.510.

   In the case of facility directories, information that may be used or disclosed is limited to the individual's name and his or her location in the facility, general condition, and religious affiliation. These provisions would permit, for example, a florist to deliver flowers to a patient in a hospital. Covered entities may disclose this information (except

for religious affiliation) to persons who ask for the individual by name. Additionally, directory information including religious affiliation may be disclosed to members of the clergy.

A covered entity may disclose certain information to a family member, relative, close friend, or other person identified by the individual. Only information directly relevant to the person's involvement with the individual's care (or payment related to the individual's health care) may be shared. If the individual objects to these disclosures (which can be an oral communication), then the covered entity is prohibited from sharing this information. These provisions also generally permit someone to act on behalf of an individual and, for instance, pick up a prescription.

PERMITTED DISCLOSURES TO FAMILY MEMBERS AND FRIENDS

A covered entity may disclose certain information to a family member, relative, close friend, or other person identified by the individual. Only the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care may be shared. If the individual is present and has the capacity to make health care decisions, the covered entity may disclose information to those involved in providing care to the individual if the covered entity does any one of the following: obtains the individual's agreement; provides the individual with the opportunity to object and the individual does not express a desire to object; or reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object. These agreements can be oral. 45 CFR §164.510(b)(2).

If an individual objects, the covered entity is prohibited from sharing health information with an individual's friends or relatives. When the individual is not present or is incapacitated, the covered entity may use its best professional judgment and experience with common practice in deciding whether a disclosure is appropriate.

Other disclosures to which individuals can agree or object are not discussed in this document; however, the reader may obtain additional information and detail in the Privacy Rule under 45 CFR §164.510. These disclosures include: (1) notification disclosures (e.g., location, general condition, or death) as set forth in 45 CFR §164.510(b)(1)(ii); (2) disclosures with respect to incapacitated persons under 45 CFR §164.510(b)(3); (3) disclosures with the individual present under 45 CFR §164.510(b)(2); and (4) disclosures for disaster relief purposes under 45 CFR §164.510(b)(4).

3) **Public Priority Purposes**

The Privacy Rule permits covered entities to use and disclose protected health information without authorization in connection with a defined list of public priority purposes. These uses and disclosures are described further in the next section of the guide. Public priority purposes include, but are not limited to, uses and disclosures required by law, for health oversight, and for public health purposes. 45 CFR §164.512.

4) **Authorization is required**

All other uses and disclosures not expressly required or permitted must have a valid prior written authorization from the individual. 45 CFR §164.508. An authorization must be:

- written in plain language;
- contain the specific information to be disclosed or used;
- identify the person(s) disclosing and receiving the information;
- contain an expiration date after which the information may not be disclosed or used;
- specify the individual's right to revoke the authorization in writing; and
- a copy of the signed authorization must be provided to the individual.

➢ **With some exceptions, a covered health care provider may not refuse treatment, and a health plan may not deny enrollment, to individuals who refuse to sign an authorization.**

Individuals have a right to request additional limitations on uses and disclosures
An individual has the right to request that the covered entity restrict uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations. The covered entity is not required to agree to such a restriction. However, if the covered entity enters into an agreement to restrict, it must abide by the agreement, except in emergency circumstances. The covered entity may terminate its agreement to restrict but only for health information created or received after it has informed the individual of the termination. An agreement to a restriction does not apply to uses or disclosures to the Secretary, to uses and disclosures for facility directories, or to uses and disclosures when an authorization or an opportunity to agree or object is not required. 45 CFR §164.522(a).

The Privacy Rule creates standards for covered health care providers and health plans to accommodate reasonable requests by individuals to receive confidential communications of protected health information from the covered entity by alternative means or at alternative locations. A covered health care provider must permit individuals to request, and must accommodate reasonable requests to receive communications of protected health information by alternative means or at alternative locations. The same standard applies to health plans, if the individual "clearly states that the disclosure of all or part of that information could endanger the individual." 45 CFR §164.522(b)(1).

Covered entities can require individuals to make requests for confidential communications in writing, and they can condition the provision of a reasonable accommodation, when appropriate, on having information as to how payment will be handled and specification of an alternative address or other method of contact. In addition, a covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis. However, a health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual. 45 CFR §164.522(b)(2).

CLIENT REQUESTS ADDITIONAL RESTRICTIONS—POTENTIAL SCENARIOS

The following are two ways that covered entities may handle a client's request for additional restrictions on the use and disclosure of protected health information. The Privacy Rule permits both responses from covered entities. In these scenarios, both physicians are covered entities.

Ruben Garcia, who is a client of Dr. Rivera, does not want his next-door neighbor, Dr. Jones, to access his protected health information and learn that he is HIV-positive. Therefore, Mr. Garcia discusses the situation with Dr. Rivera who agrees to restrict access to Mr. Garcia's records. Because Drs. Rivera and Jones work in a large AIDS services organization that already has several controls on who can access information, Dr. Rivera believes that he can honor this request without undue difficulty. Further, he believes that if he refuses Mr. Garcia's request, it could hinder the trust they have established and it could cause Mr. Garcia to stop seeking care. Therefore, he enters into a written agreement with Mr. Garcia saying that he will restrict access to Mr. Garcia's medical records so that only specifically identified providers are able to access them.

****

Maya Johnson has heard that Dr. Baker has a reputation of being particularly sensitive to the needs of women with HIV. On her first visit, however, she sees that someone she knows from church, Penny Schmidt, is the office manager and manages the billing process. Ms. Johnson wants to see Dr. Baker, but she doesn't want Ms. Schmidt to see the details of the types of medical care she is receiving. She requests that Dr. Baker restrict access to prevent Ms. Schmidt from seeing her protected health information. Because Dr. Baker is in a small practice, all client records are maintained in paper files and Ms. Schmidt is the sole person responsible for billing. While she would like to honor Ms. Johnson's request, she does not believe that she could do so. Therefore, she refuses Ms. Johnson's request to restrict.

Covered entities are permitted to seek consent to use and disclose protected health information for treatment, payment, and health care operations purposes.

Providing consent for the use or disclosure of protected health information for treatment, payment, and health care operations is not the same as providing authorization to use and disclose protected health information for other purposes. A covered entity may, at its discretion, obtain the individual's consent to use or disclose protected health information for treatment, payment, and health care operations, although the Privacy Rule does not require a covered entity to obtain consent for these uses. Covered entities that choose to obtain consent have discretion in designing the consent form and developing a procedure for obtaining consent. If the covered entity means to use or disclose information for some purpose other than treatment, payment, or health care operations, and the regulation provides no other basis for that use or disclosure, the consent just discussed is not adequate. The entity must obtain an authorization which meets the requirements in the Privacy Rule. Moreover, this *consent* is not the same as providing informed consent for treatment. 45 CFR §164.506(b).

Interaction of the Privacy Rule with state laws and regulations

The Privacy Rule establishes a Federal *floor* of legal protection for health information that leaves other, stronger protections of state law in place. The protections are cumulative, so that the individual gets the strongest protections and benefits of each law. 45 CFR §160.203. State laws that are not contrary to the Privacy Rule remain in effect. State laws that are contrary to the

Privacy Rule and that are less stringent are preempted. State laws related to the privacy of health information that are more stringent than the Privacy Rule will remain in effect when they are contrary to the Privacy Rule. Generally, a state law is *more stringent* when it provides greater privacy rights for the individual who is the subject of the information. 45 CFR §160.202 and 45 CFR §160.203.

Grantees are already familiar with the many state laws that provide special protections for HIV/AIDS test results and other HIV/AIDS related information, and those laws are often more protective than the Privacy Rule. They may, for example, require a separate authorization to disclose such information. Or both the Privacy Rule and state law may permit a particular disclosure without authorization, but the state law may impose some conditions on the disclosure, or limit to whom the disclosure may be made.

It is important that grantees be aware of both the Privacy Rule and the state law applicable to their activities, and develop policies and procedures that ensure their clients receive all the protections under both. It may be necessary to consult with legal counsel to resolve particular issues about the relationship of the Privacy Rule to state law.

Many state laws require reporting or other disclosure of information about patients. The Privacy Rule permits any disclosure that is required by law. 45 CFR §164.512(a). Thus, required disease or injury reporting, vital events reporting, and reporting of abuse of any person, are all permitted disclosures under the Privacy Rule. Likewise, the Privacy Rule permits health plans to comply with laws that require reporting or granting access to information to state agencies for audits, evaluation, or licensure.

In this regard it should be noted that many disclosures referenced here are permitted by the Privacy Rule even without an actual obligation to report or disclose under state law. For example, the provisions relating to disclosures for oversight and public health purposes, as discussed below in Section 5, permit many of these disclosures; the state law need not require the disclosure, nor need the state official obtain a court order, for a covered entity to properly disclose information for these purposes, as long as the Privacy Rule's conditions for the particular disclosure are met.

RECOMMENDED ACTIONS

1) Conduct an audit of all of the ways that protected health information is routinely used or disclosed, in order to determine in which category the use or disclosure falls.

2) Develop policies and procedures for implementing the use and disclosure requirements for each category.

3) Develop policies and procedures for handling disclosures to family members, close friends, and associates.

4) Develop policies and procedures for evaluating and implementing requests from individuals for additional restrictions on uses and disclosures of their protected health information.

5) Determine whether you or your organization will elect to seek consent to use and

disclose protected health information for treatment, payment, or health care operations. Establish policies and procedures to implement your organization's decision.

6) Review existing state laws and other Federal laws applicable to your program to determine if they contain additional requirements or restrictions on uses and disclosures or greater rights of access of protected health information. The Attorney General's office in your state may serve as a good resource for determining which state laws interact with the Privacy Rule.

5. What disclosures are permitted without individual authorization?

In addition to uses and disclosures to the individual who is the subject of the information and for treatment, payment, and health care operations, uses and disclosures can be made for the following public priority purposes without individual authorization:

PERMITTED PUBLIC PRIORITY DISCLOSURES WITHOUT INDIVIDUAL AUTHORIZATION

As described in this section, disclosures are permitted without first obtaining an individual's authorization for certain purposes. There are requirements that must be met and/or limitations that are imposed for most of these disclosures. These disclosures include:

-- When required by law;

-- Health oversight activities;

-- Public health authorities for public health activities;

-- When responding to an imminent threat to any person or the public;

-- Disclosures in connection with abuse, neglect, or domestic violence;

-- Workers Compensation;

-- When responding to court orders or other legal process;

--To law enforcement;

-- Certain research activities;

-- Specialized government functions;

-- Decedents; and

-- Cadaveric organ, eye, or tissue donation.

See 45 CFR §164.512 for a complete description of each permitted disclosure.

When required by law

A covered entity may use or disclose protected health information to the extent that the law requires it and the disclosure complies with, and is limited to, the relevant requirements of such law. 45 CFR §164.512(a). Although other permitted disclosures are limited by the *minimum necessary* standard, this standard does not apply to disclosures required by law.

- **If Ryan White CARE Act grantees are required to report names of clients under public health reporting laws, the Privacy Rule permits these disclosures.**

Health oversight activities

Disclosures may be made to health oversight agencies as defined in the Privacy Rule for oversight activities authorized by law, including, but not limited to: audits; civil, administrative, or criminal investigations; inspections; and licensure or disciplinary actions. 45 CFR §164.512(d). Such disclosures are subject to the Privacy Rule's minimum necessary requirement. This provision does not encompass investigations of individuals that are not related to the receipt of health care, not related to claims for public benefits related to health care or not related to qualification for public benefits when an individual's health is integral to the claim. Ryan White CARE Act grantees are subject to audit by the HHS Office of the Inspector General (OIG). The OIG is a health oversight agency and its audits, investigations and/or inspections of the Ryan White CARE Act grantees and sub-grantees are health oversight activities for which disclosure of protected health information is permitted by the Privacy Rule.

Public health purposes

A covered entity may disclose protected health information for certain *public health activities* to certain specified recipients. These include public health authorities (such as HRSA, the Centers for Disease Control and Prevention, the Food and Drug Administration, the Occupational Safety and Health Administration, and state public health agencies, when they are operating as a public health authority), persons subject to the jurisdiction of the Food and Drug Administration, and to persons exposed to a communicable disease (if other laws authorize such notification). 45 CFR §164.512(b). Additionally, in certain circumstances involving workplace health and safety laws, a covered health care provider may disclose protected health information for certain purposes to an employer about an individual who is a member of that employer's workforce. Disclosures for public health purposes are subject to the Privacy Rule's minimum necessary requirement.

- **Some reporting required by HAB is permitted under either the health oversight or public health exceptions. The exception that applies depends on the purpose for which the information is collected.**

A covered entity may also create a *limited data set* which may be used or disclosed for public health, research or health care operations purposes without authorization pursuant to a valid data use agreement. 45 CFR §164.514(e).

LIMITED DATA SET

A covered entity may create and share a *limited data set* that it may use or disclose for health care operations, public health, and research purposes without individual authorization.

A limited data set, while not considered de-identified information, has the following direct identifiers of the individual (or relatives, employers or members of the individual's household) removed: name; postal address information other than city, state and zip code; account numbers and biometric identifiers; social security number; telephone and fax number; e-mail address; full face photo; medical record number; and a few others. For instance, a covered HIV services provider could share a limited data set with a health department in order for it to aggregate and analyze data from many services providers in a community to monitor trends in HIV and Hepatitis C co-infections.

The Privacy Rule conditions use or disclosure of the limited data set on a covered entity's entering into a data use agreement with the recipient, in which the recipient agrees to: limit the use of the data set for the purposes for which it was given; ensure the security of the data; report breaches of the agreement of which it becomes aware; ensure that its agents and subcontractors agree to the same restrictions and conditions that apply to the recipient; and not re-identify the information or use it to contact any individual.

If the data recipient is a covered entity and it knowingly violates a data use agreement, it is in noncompliance with the Privacy Rule (see 45 CFR §164.514(e)(4)(iii) for details). If the data recipient is not a covered entity, HHS cannot take enforcement activity directly against it, but can against the covered entity that entered into the agreement.

When responding to an imminent threat to any person or the public

Consistent with applicable law and standards of ethical conduct, a covered entity may use or disclose protected health information if the covered entity, in good faith, believes that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is to a person reasonably able to prevent or lessen the threat, which could include the target of the threat, or that the disclosure is necessary for law enforcement authorities to identify or apprehend an individual under certain circumstances. 45 CFR §164.512(j).

Disclosures in connection with abuse, neglect, or domestic violence

A covered entity may disclose information about individuals believed to be victims of abuse, neglect, or domestic violence to a government authority to the extent the disclosure is required by law, or if the individual agrees to such disclosure. 45 CFR §164.512(c). Additionally, a covered entity may disclose this type of information if such a disclosure is expressly permitted by a law or statute and certain specified criteria are met. Special provisions apply when the individual is unable to agree to the disclosure because of incapacity or when disclosure is needed to prevent serious harm. Disclosures related to possible child abuse may only be made to public health authorities or appropriate government agencies authorized by law to receive reports of child abuse or neglect.

Workers Compensation

A covered entity may disclose protected health information as authorized by laws relating to workers' compensation or other similar programs. Workers' compensation carriers are not

considered health plans under the Privacy Rule, and are, therefore, not covered entities under the Privacy Rule. 45 CFR §164.512(*l*).

When responding to court orders or other legal process

The Privacy Rule allows a covered entity to disclose protected health information in response to an order of a court or administrative tribunal, but only to the extent the information is covered by the order. Furthermore, a covered entity may disclose protected health information in response to a subpoena, discovery request, or other lawful process if the covered entity receives satisfactory assurance that the party seeking the information has made reasonable efforts to ensure that the individual who is the subject of the requested information has been given notice of the request or a protective order has been sought for the information. 45 CFR §164.512(e).

DISCLOSURES TO LAW ENFORCEMENT

A covered entity may disclose protected health information in certain circumstances to law enforcement officials. Permissible circumstances are described in the Privacy Rule in 45 CFR §164.512(f). Disclosures may be made to law enforcement officials in the following circumstances:

-- Pursuant to process (such as a court order, a court-ordered warrant or a judicial subpoena) or when required by law

-- Limited information for purposes of identification and location of a suspect, fugitive, material witness or missing person

-- Information about an individual suspected to be a victim of a crime

-- Decedents if death may have resulted from a criminal action

-- Crime on the covered entity's premises

-- Reporting crime in emergencies

Research

It is important to note that the Privacy Rule does not apply to research; it applies to covered entities, which researchers may or may not be. For example, when researchers also are health care providers who conduct certain electronic transactions, they are subject to the Privacy Rule as covered entities. When they work or volunteer for covered entities (e.g., researchers within certain academic medical centers), researchers may be required by the covered entity to comply with the Privacy Rule. Other researchers may also collect, use, and release individually identifiable health information, but they will not qualify as covered entities if they are not health care providers who conduct certain electronic transactions. Unlike the applicability of the HHS Protection of Human Subjects Regulations at 45 CFR part 46 to institutions that engage in human subjects research conducted or supported by the HHS, the source of funding does not determine whether an individual or entity is a *covered entity* and, therefore, subject to the Privacy Rule. Some researchers may find themselves having to comply with both sets of regulations.

The Privacy Rule describes the ways in which covered entities can use or disclose protected health information for research purposes. 45 CFR §164.512(i). In general, the Rule allows covered entities to use and disclose protected health information for research if authorized to do so by the subject in accordance with the Privacy Rule. However, to gain access for research purposes to protected health information created or maintained by covered entities without an individual's authorization, a researcher may have to provide supporting documentation on which the covered entity may rely in compliance with the Privacy Rule. For example, protected health information can be used or disclosed for research if a covered entity obtains documentation that an Institutional Review Board (IRB) or another review body called a Privacy Board has waived the requirement for authorization or allowed an alteration. The Rule also allows a covered entity to enter into a data use agreement for sharing a limited data set for research purposes (discussed previously). There are also separate provisions for how protected health information can be used or disclosed for activities preparatory to research and for research on decedents' information. Additional information on the Privacy Rule and research can be found at:

http://privacyruleandresearch.nih.gov

IRBs and Privacy Boards

The Privacy Rule permits a covered entity to use or disclose the protected health information for research without authorization if it obtains documentation that an IRB or Privacy Board has waived or altered the authorization requirement. Under the Privacy Rule, either board may waive or alter the Privacy Rule's authorization requirements for the use and disclosure of protected health information if the board determines that certain criteria for waiving or altering the authorization requirement have been met. A Privacy Board is a review body that may be established to review and, if appropriate, approve requests for a waiver or an alteration of the authorization requirement under the Privacy Rule for uses and disclosures of protected health information for the research. Privacy Boards, however, do not exercise any of the other powers or authority granted to IRBs under Federal laws relating to federally-conducted or supported human subjects research and research involving products regulated by the Food and Drug Administration (FDA). The Privacy Rule is specific with regard to how the Privacy Board should be composed. For example, it requires that at least one member not be affiliated with the entity sponsoring the research. The Privacy Rule does not alter IRB membership requirements, jurisdiction on matters concerning the protection of human subjects, or other procedural IRB matters.

Review criteria

A covered entity may use and disclose protected health information, without an authorization, or with an altered authorization, if it receives the proper documentation of approval of such alteration or waiver from an IRB or a Privacy Board. Many of the waiver criteria of the Privacy Rule were modeled on the HHS Protection of Human Subjects Regulations. In order for a covered entity to use or disclose protected health information under a waiver or an alteration of the authorization requirement, it must receive documentation of, among other things, the IRB or Privacy Board's determination that the PHI use or disclosure involves no more than minimal risk to the privacy of

individuals due, in part, to an adequate plan to protect protected health information identifiers from improper use and disclosure. (Complete waiver criteria can be found at 45 CFR §164.512(i)(2)(ii)). Such a determination may be made during the normal, convened session of the IRB or Privacy Board or through expedited review if the IRB or Privacy Board has determined that there is no more than minimal privacy risk to the individual. Expedited review allows the chair of the IRB or Privacy Board or a designee to approve the waiver alone, rather than by a vote of the convened board.

Preparatory to research activities and research on decedents

The Privacy Rule allows protected health information to be used and disclosed for research without either an authorization or waiver of the authorization requirement when the activity is considered preparatory to research or is research on decedents' protected health information. For example, the Privacy Rule allows a covered entity to use and disclose to a researcher protected health information to prepare a research protocol or some other activity in preparation for research, including aiding in study recruitment. In addition, research solely on a decedent's protected health information is permitted without authorization from the individual or his/her personal representative or waiver of authorization. In both situations, certain conditions must be met before the covered entity is permitted to disclose protected health information for these purposes. See 45 CFR §164.512(i)(1)(ii) for conditions relating to preparatory to research activities and 45 CFR §164.512(i)(1)(iii) for conditions relating to research on decedents' information.

Specialized Government Functions

An authorization is not required to use or disclose protected health information for specialized government functions, such as: 1) certain military, intelligence and national security activities; 2) to assure protection of the President and others; 3) certain disclosures by the Department of State to Department of State officials regarding medical suitability determinations; 4) certain disclosures to a correctional institution or other law enforcement custodial situations; and 5) for eligibility or enrollment information by a government health plan to another agency that administers a government program providing public benefits if required or expressly authorized by statute or regulation. See 45 CFR §164.512(k) for a complete description of these and other permitted disclosures for specialized government functions.

Decedents

Protected health information may be disclosed without prior authorization to funeral directors, coroners or medical examiners to carry out their occupational duties or other duties authorized by law. 45 CFR §164.512(g).

Cadaveric Organ, Eye, or Tissue Donation

Protected health information may be disclosed to organ procurement organizations or entities engaged in organ, eye, or tissue procurement, banking, or transplantation to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue. 45 CFR §164.512(h).

6. Other provisions regarding uses and disclosures of protected health information.

ADDITIONAL PERMITTED DISCLOSURES WITH SPECIFIC REQUIREMENTS

As described in this section, additional disclosures are permitted but must comply with specific requirements. These disclosures include:

-- Certain fundraising;

-- To business associates; and

-- Marketing activities.

Fundraising

A covered entity may use and disclose protected health information of an individual without the individual's authorization to raise funds for its own benefit if the proposed fundraising meets certain criteria. 45 CFR §164.514(f). The information used or disclosed must be limited to demographic information related to an individual and the dates of health care provided to an individual:

- If the institution is not doing the fundraising in-house, it can only disclose the information to a business associate or an institutionally related foundation;
- The covered entity must specifically note that it uses information for fundraising purposes in its notice of privacy practices;
- Any fundraising materials must include a description of how the individual can opt out of future fundraising communications; and
- The covered entity must make reasonable efforts to ensure that an individual who has exercised his or her opt-out rights does not receive further fundraising materials.

Because fundraising is included in the definition of *health care operations*, an individual has the right to request in advance that a covered entity restrict uses and disclosures for such purposes. However, the covered entity is under no obligation to agree to such a restriction.

Business Associates

Health plans and providers routinely contract with other companies and consultants to perform a wide variety of functions on their behalf. Health plans and providers, for example, may work with outside attorneys, bill collectors, computer specialists, or accreditation organizations. All of these entities may need access to protected health information to perform their jobs on a client's behalf. But these persons or entities are generally not directly subject to the Privacy Rule. To allow information to be shared with these *business associates* and to protect information that may be disclosed to them, the rule establishes specific conditions on when and how covered entities may share information with these entities. 45 CFR §164.502(e) and §164.504(e).

A *business associate* is a person or entity who, on behalf of a covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, such as:

- claims processing or administration;
- data analysis;
- utilization review;
- quality assurance;
- billing;
- practice management; or,
- providing legal, actuarial, accounting consulting, data aggregation, management, administrative, accreditation, or financial services.

A business associate does not include a member of the covered entity's workforce. Neither does it include the circumstance where two covered entities participate in an organized health care arrangement, such as a hospital where a doctor has privileges. 45 CFR §160.103. A covered entity may disclose protected health information to a health care provider concerning treatment of an individual without creating a business associate relationship. Furthermore, the Rule is not intended to cover the provision of protected health information to a person who merely acts as a conduit for protected health information, such as the U.S. Postal Service, nor to persons or entities whose access to protected health information is merely incidental.

- **A covered entity is permitted to disclose protected health information to a business associate or to allow the business associate to create or receive protected health information on its behalf if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.**

Generally, these satisfactory assurances must be in a written contract which, among other things, requires the business associate not to use or disclose the information other than as permitted or required by the contract or as required by law, and to implement appropriate safeguards to prevent inappropriate uses and disclosures. A contract is not required in certain circumstances where the covered entity and the business associate both are governmental agencies or where the business associate is required by law to perform the business associate function. In these cases, certain alternative documentation may be required.

EXTENDED TIMEFRAME TO COMPLY WITH CONTRACT REQUIREMENTS

Covered entities other than small health plans may have up to one additional year to comply with the business associate contract requirements of the Privacy Rule. 45 CFR §164.532(d). Specifically, providers will have a maximum of an additional year (until April 14, 2004) to conform existing contracts with the Privacy Rule's contracting requirements if the provider's existing contracts were entered into prior to October 15, 2002 and were not renewed or modified prior to April 14, 2003.

This one-year grace period is a maximum. If a contract is renewed or modified between April 14, 2003, and April 14, 2004, then the contract must be compliant by the renewal or modification date. Contracts with business associates that were entered into on October 15, 2002, or later, or that were renewed or modified between October 15, 2002, and April 14, 2003, must comply with the Privacy Rule's specifications as of April 14, 2003.

Marketing

The Privacy Rule requires a covered entity to obtain an individual's prior written authorization to use or disclose protected health information for marketing. 45 CFR §164.508(a)(3).

Under the Privacy Rule, *marketing* means (1) to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, or (2) an arrangement between a covered entity and any other entity in which the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service. 45 CFR §164.501.

The Privacy Rule expressly excludes various types of communications from the definition of marketing. The types of communications excluded from the definition include: those that describe a health-related product or service that is provided by, or included in a plan of benefits of, the covered entity making the communication; those that describe the entities participating in a provider or plan network of the covered entity making the communication; those that describe replacement of or enhancements to, a health plan; those that describe health-related products or services available only to health plan enrollees that add value to (but are not part of) the plan's benefits of the covered entity making the communication; those for treatment of the individual; those made for case management and care coordination for the individual; and those made to direct or recommend alternate treatments therapies, providers, or settings of care to the individual.

Thus, communications from a covered entity to an individual that are related to the treatment of the individual are **not** marketing under the Privacy Rule, so they do not require prior written authorization.

- **No authorization is required if a pharmacy conducts its own review of its prescription records and mails letters to individuals on antiretroviral therapy encouraging them to switch their medication to another drug manufacturer's product if the purpose of the activity is for treatment or to recommend alternative therapies to the individual. If the drug manufacturer of the product pays the pharmacy to perform this activity, the pharmacy may still perform this activity without an individual authorization.**

RECOMMENDED ACTIONS

1) Develop policies and procedures for handling each of the described uses and disclosures.

2) Consider whether there are uses and disclosures for health care operations, public health, or research where a limited data set could be used.

3) Identify all business associates and execute written contracts with each of them. See sample business associate contract provisions provided by the Office for Civil Rights - available at : http://www.hhs.gov/ocr/hipaa/contractprov.html.

7. How much information can be used and disclosed?

There are a couple of specific requirements related to the use and disclosure of information.

Minimum necessary requirement

In most cases, whenever a covered entity uses or discloses protected health information or requests such information from another covered entity, it must make reasonable efforts to limit the information to the minimum amount necessary to accomplish the intended purpose of the use or disclosure. 45 CFR §164.502(b) and 45 CFR §164.514(d). In the context of treatment, the minimum necessary standard applies only to uses of protected health information. Disclosures for treatment purposes are not subject to this standard.

- **The minimum necessary standard does not apply to disclosures to or requests by a health care provider for treatment purposes. Neither does the standard apply to disclosures made to individuals pursuant to their request, to those made to the Secretary for overseeing compliance of the Privacy Rule, to uses or disclosures that are required by law, or to uses or disclosures pursuant to an authorization.**

Psychotherapy notes are afforded heightened protections

Psychotherapy notes are afforded special treatment and heightened protection. For most purposes, a covered entity may not use or disclose information contained in psychotherapy notes without an authorization from the individual that meets the Privacy Rule's requirements. Such an authorization must specify, among other requirements, who is authorized to receive the information and include an expiration date or event. 45 CFR §164.508(a)(2).

Psychotherapy notes are limited to those notes that are recorded by a mental health professional documenting or analyzing the contents of conversations during counseling sessions and that are separated from the rest of the individual's medical record. 45 CFR §164.501.

The diagnosis (or disease code) and certain other information, including prescribed medications, are not considered to be psychotherapy notes and may be disclosed for treatment, payment, or health care operational purposes.

- **The Privacy Rule prohibits a covered health care provider or a health plan from conditioning treatment, payment, enrollment in the health plan, or the provision of benefits on the individual's authorization for the release of psychotherapy notes.**

RECOMMENDED ACTIONS

1) Develop policies and procedures for determining what constitutes the *minimum necessary* for all routine uses and disclosures of protected health information.

2) If you (or your organization) use or develop psychotherapy notes, you should establish policies and procedures for appropriately safeguarding this information.

8. What is the impact of the Privacy Rule on information sharing or reporting with HRSA's HIV/AIDS Bureau (HAB)?

It is anticipated that the Privacy Rule will have a minimal direct impact on HAB operations. HAB does not meet the Privacy Rule's definition of a covered entity. Therefore, HAB is not subject to the Privacy Rule. Nonetheless, HAB remains subject to the Federal Privacy Act.

Under the Privacy Rule, a covered entity may disclose protected health information without the individual's authorization for health oversight activities and public health activities and purposes to authorities authorized by law to collect or receive such information. Some data reporting required by HAB is permitted by the Privacy Rule without individual authorization by the health oversight exception and/or public health exception, depending on the purpose for which the information is collected. For example, in making grants, HAB is required to monitor and assess those grants through evaluation activities under Section 241 of the Public Health Service (PHS) Act and the Uniform Administrative Requirements for grants. Disclosure of protected health information by covered entities to HAB for this purpose is permitted under the health oversight exception (45 CFR §164.512(d)). In other circumstances, HAB is authorized by law to collect information for monitoring trends in the HIV epidemic, such as demographic data in applications for funding under the Ryan White CARE Act. (See the following sections of the PHS Act: 2605(b), 2613(c), 2617(b)(2), and 2664(a)(2)). Disclosure of protected health information by covered entities to HAB for this purpose is permitted under the public health activity exception (45 CFR §164.512(b)).

IMPACT ON CLIENT DEMONSTRATION PROJECTS (CDPs)

HAB funds Client Demonstration Projects (CDPs). These projects have established their own Institutional Review Board (IRB) processes.

Disclosures for research can be made without authorization if the covered entity receives appropriate documentation that an Institutional Review Board (IRB) or privacy board waives in whole or in part the individual authorization requirement. An existing IRB established in accordance with the Common Rule (or FDA regulations) that regulates federally funded research or FDA human subject protection regulations may perform this function. The Privacy Rule includes specific requirements for establishing privacy boards.

Privacy Board Composition

Privacy boards must:

-- Have members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests

-- Include at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with such entities

-- Not have any member participating in a review of any project in which the member has a conflict of interest

Required Documentation

For documentation of a waiver of authorization to be sufficient to permit a covered entity to use or disclose protected health information for research based thereon, it must contain: (1) a statement identifying the IRB or privacy board; (2) the date on which the alteration or waiver was approved; (3) a statement that the IRB or privacy board has determined that the alteration or waiver satisfies the applicable criteria used to evaluate the request for alteration or waiver; (4) a brief description of the protected health information that is needed; (5) a statement that the alteration or waiver has been reviewed under either normal or expedited review procedures; and (6) the required signature(s).

- **Ryan White CARE Act grantees may be required to report certain information to HAB or other HHS agencies, as a condition of grant award. When this information is being collected in order to perform program and grant administration functions, these disclosures are permitted by the Privacy Rule without individual authorization as health oversight activities, subject to the minimum necessary requirements.**

- **Ryan White CARE Act grantees may be required to report certain information to HAB, as a condition of grant award. When this information is being collected in order to monitor trends in the HIV epidemic, the Privacy Rule permits these disclosures without individual authorization as a public health purpose, subject to the minimum necessary requirements.**

RECOMMENDED ACTIONS

1) Organizations that are covered entities with Client Demonstration Projects (CDPs) should evaluate their IRB procedures to determine whether they comply with the Privacy Rule's requirements.

2) Organizations that are covered entities and work with CAREWare developers should ensure they execute business associate contracts with these developers.

9. What steps must covered entities take to comply with the Privacy Rule?

The Privacy Rule is intended to be flexible and scalable…how a three-person physician's office must implement the rules can be very different from how a hospital with 3,000 employees must implement them.

REQUIRED ACTIONS

In order to be in compliance with the Privacy Rule, covered entities must, among other requirements:

1) Designate a privacy official

2) Designate an individual who serves as a contact person to receive complaints

3) Develop policies and procedures as described throughout this guide and for receiving and addressing complaints

4) Train members of the workforce

5) Put in place appropriate technical, administrative, and physical safeguards to protect the privacy of protected health information

6) Develop sanctions for employees who violate privacy policies

7) Document personnel decisions, policies, training, sanctions, and complaints

10. How is the Privacy Rule enforced?

The approach of the Office for Civil Rights (OCR) to compliance and enforcement is, whenever possible, to work cooperatively with covered entities to achieve voluntary compliance. Additionally, OCR is committed to assisting covered entities in complying with the Privacy Rule through the provision of technical assistance.

Any person who believes a covered entity is not complying with the applicable requirements of the Privacy Rule may file a complaint with the covered entity or with the Secretary. 45 CFR §164.530(d) and §160.306. A person includes an individual person, as well as any type of association, group, or organization.

Complaints

There are three requirements for filing a complaint with the Secretary:

1) The complaint must be filed in writing, either on paper or electronically;
2) The complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be violations of the Privacy Rule; and,
3) The complaint must be filed within 180 days of when the complainant knew (or should have known) of the violation of the Privacy Rule. The Secretary has the authority to waive the time limit if there is a showing of good cause.

The complaint procedure and a sample complaint form is available at:

www.hhs.gov/ocr/privacyhowtofile.htm.

OCR is authorized to conduct an investigation of the complaint. This investigation may include review of relevant policies, procedures, and practices of the covered entity and the specific circumstances of the complaint. After an investigation, OCR will notify the covered entity and the complainant of the outcome of the investigation. If there is an indication of noncompliance, OCR will, whenever possible, attempt to resolve the matter informally.

Compliance Reviews

The Privacy Rule authorizes OCR to conduct compliance reviews to determine whether covered entities are complying with the Privacy Rule. 45 CFR §160.308. While OCR has authority to conduct compliance reviews, for the foreseeable future, its formal enforcement activities will primarily be complaint investigations. As with the investigation of a complaint, OCR will notify the covered entity of the outcome of the review. If there is an indication of noncompliance, OCR will, whenever possible, attempt to resolve the matter informally.

The Privacy Rule places three responsibilities on covered entities with regard to compliance:

1) Provide records and compliance reports in a timely manner, and containing such information as the Secretary determines to be necessary;
2) Cooperate with complaint investigations and compliance reviews; and
3) Permit access to information.

Under normal circumstances, a covered entity must permit OCR, during normal business hours, to access its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the Privacy Rule. Under exigent circumstances, such as when documents may be hidden or destroyed, a covered entity must permit access by OCR at any time without notice. Protected health information that is obtained by OCR in connection with an investigation or compliance review will not be disclosed by OCR unless it is necessary for ascertaining or enforcing compliance with the Privacy Rule, or it is otherwise required by law.

Penalties

The Administrative Simplification provisions of HIPAA establish civil and criminal penalties for violations of the Privacy Rule. There is a civil money penalty per violation of up to $100, which is capped at a maximum of $25,000 per calendar year, for violations of an identical requirement or prohibition. Criminal penalties may be imposed for certain wrongful acts, which escalate to a maximum of $250,000 and ten years imprisonment for particularly egregious offenses. HIPAA does not create a Federal right to sue for violations of the Privacy Rule.

Acknowledgements

The following individuals provided extensive time, effort and dedication to the development of this document:

Jeffrey S. Crowley, MPH
Project Director
Georgetown University
Institute for Health Care Research and Policy

Ivana R. Williams, MPA, RPT (Government Project Officer)
Senior Program Management Consultant
Office of Policy and Program Development
Department of Health and Human Services (DHHS)
Health Resources and Services Administration (HRSA)
HIV AIDS Bureau

Melissa Bartlett, J.D.
Privacy Program Specialist
DHHS, Office for Civil Rights

Sandra Karen
System Analyst
Division of Knowledge Management
DHHS, HRSA, Office of Information Technology

Lora Kutkat, M.S.
Health Science Policy Analyst
Office of Science Policy and Planning
DHHS, National Institutes of Health
Office of the Director

Elizabeth H. Saindon, J.D.
Senior Attorney
DHHS, Office of the General Counsel
Public Health Division

Jessica Townsend
Senior Staff Fellow
DHHS, HRSA
Office of Planning and Evalutation