HEALTH PRIVACY PROJECT

INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

Summary of HIPAA Privacy Rule

Prepared by: Health Privacy Project
Institute for Health Care Research and Policy
Georgetown University
2233 Wisconsin Avenue, NW
Suite 525
Washington, DC 20007
202-687-0880
www.healthprivacy.org

Staff contacts: Joy Pritts, Senior Counsel
Joanne Hustead, Senior Counsel
Angela Choy, Field Director

September 13, 2002

HEALTH PRIVACY PROJECT
INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

Summary of HIPAA Privacy Rule

Table of Contents

I. Background

A. Health Insurance Portability and Accountability Act

The 1996 Health Insurance Portability and Accountability Act (HIPAA) included a deadline for enacting federal health privacy rules. HIPAA required that if Congress failed to pass comprehensive health privacy legislation by August 21, 1999, the Secretary of Health and Human Services (HHS) must issue regulations.

Despite the introduction of numerous proposals, Congress failed to meet its deadline. As required under HIPAA, the Secretary of HHS issued the health privacy regulation in December 2000. (See timeline below.) On August 9, 2002, HHS issued significant modifications to the regulation. The regulation has the force of law. Under HIPAA, HHS cannot issue further modifications to the regulation until August 2003.

This paper provides a summary of the privacy regulation, incorporating the recent modifications. While the regulation provides important new privacy protections for health care consumers, it is not comprehensive. As provided for by HIPAA, the regulation will only directly apply to health plans, health care clearinghouses, and certain health care providers. Only Congress has the authority to pass a comprehensive federal law that will directly cover *all* of the entities that collect, maintain, and disclose health information – such as life insurers and pharmaceutical companies.

It is also important to note that the privacy regulation is part of a package of regulations mandated in HIPAA. The package includes privacy, security, and electronic transaction standards. Taken together, they are designed to facilitate the development of a uniform, computer-based health information system, while protecting the privacy of consumers.

B. Timeline

November 3, 1999:	Draft rules published in the *Federal Register.*
February 17, 2000:	Public comment period closes. HHS received more than 52,000 comments on the draft.
December 28, 2000:	The final regulation is published in the *Federal Register*.
April 14, 2001:	The regulation is *effective,* but covered entities do not yet have to comply with the regulation.
July 6, 2001:	HHS issues guidance on the regulation.

March 20, 2002:	HHS proposes modifications to the privacy regulation with a 30-day comment period.
August 14, 2002:	Final modifications to the regulation are published in the *Federal Register*.
October 15, 2002:	The modifications to the regulation are scheduled to take effect. Compliance is not yet required.
April 14, 2003:	Covered entities must be in compliance with the regulation, except small health plans.
April 14, 2004:	Small health plans must be in compliance with the regulation.

C. About the Summary

This summary provides a broad overview of the major provisions of the regulation. It does not, however, follow the organization of the regulation itself. Rather, it is organized by topics of interest.

In order to help users find particular provisions in the regulation itself, citations for particular provisions are included. The Health Privacy Project has posted an unofficial text of the regulation as of August 14, 2002, on its Web site, at http://www.healthprivacy.org. At some point, an official version of the regulation will be published in Volume 45, Parts 160 and 164 of the Code of Federal Regulations (CFR).

II. Scope of Coverage

A. Who is Covered?

§ 160.102; § 160.103; § 164.104; and § 164.500

The regulation applies to health plans, health care clearinghouses, and to health care providers who transmit health information in electronic form in connection with specified financial and administrative transactions (such as claims for payment). These persons and organizations are referred to as **"covered entities"** in the regulation.

Health plan

The definition of "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 high-risk pools are specifically covered.[1] Most employee health benefit plans are covered. However, *employers* who sponsor these group health plans are *not* covered entities under the regulation. (See "Group Health Plans" for a discussion of when and how protected health information may be shared with employers.)

Additionally, the rule specifically *excludes* certain entities that provide or pay for health care. For example, small employee health benefit plans (fewer than 50 participants) that are self-administered are exempt from the rule. Likewise, workers' compensation carriers are excluded from the definition of health plan. Government-funded programs that only incidentally provide or pay for the cost of health care are not health plans. Government-funded programs that have as their principal purpose the provision of health care are also not health plans, but they may meet the definition of health care provider.

Health care clearinghouse

"Health care clearinghouse" is a term of art under the regulation, and differs somewhat from the manner in which the term is generally used. Under the regulation, a health care clearinghouse is an entity that translates health information received from other entities either to or from the standard format that will be required for electronic transactions. For instance, a health provider may submit claims information to a health care clearinghouse to process that information into a standard format for submission to a health plan.

Health care provider who electronically transmits health information in standard format

The regulation covers health care providers who transmit health information electronically in a "standard format" in connection with HIPAA standard transactions. Determining whether a person or organization comes within this category entails applying a three-prong test: 1) Is the person or organization a "health care provider" as defined in the regulation? 2) Do they transmit health information electronically in connection with one of the financial or administrative transactions specified in HIPAA? *and* 3) Is that health information transmitted in a standard electronic format?

1. Health care provider

For purposes of the regulation, "health care provider" includes any person or entity that furnishes, bills, or is paid for health care in the normal course of business. "Health care," in turn, is broadly defined as "care, services, or supplies related to the health of an individual." Thus, the term health care provider includes both persons (such as dentists and podiatrists) and entities (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 regulation also covers both the providers of care and services (such as practitioners) and the providers of health supplies (such as pharmacists and hearing aid dispensers). However, the regulation is not intended to encompass blood banks, sperm banks, organ banks, and similar organizations.

2. Transmitting health information electronically in connection with standard transactions

To transmit health information electronically, a provider must transfer personally identifiable health information via computer-based technology. Using the Internet, an Intranet, or private network system will bring a provider within the reach of the regulation. Similarly, transferring information from one location to another using magnetic tape or disk is the type of electronic transmission included in the regulation. In contrast, sending information via telefax is not considered to be transmitting information electronically.

To come within the scope of the regulation, the health information must be transmitted in connection with one of the financial and administrative transactions listed in Section 1173 of HIPAA. These transactions include, but are not limited to, health claims, determining enrollment and eligibility in a health plan, and referral authorization.[2] Providers who directly submit health claims electronically clearly come within the regulation. Even providers who rely on third-party billing services to conduct such electronic transactions on their behalf are covered under the regulation.

In contrast, providers who operate solely on a paper basis and do not submit insurance claims electronically will not be subject to the regulation. For instance, an Internet pharmacy that *only* accepts credit card payments will not be covered by the privacy regulation. If this Internet pharmacy submits insurance claims electronically, however, then it would be covered by the regulation.

3. Transmitting information in the required "standard format"

A provider that transmits health information electronically in relation to any of the standard transactions, such as verifying insurance coverage or filing a health claim, must use a standard electronic format (*i.e.,* the provider must include certain information and use specified codes for diagnosis and treatment) required by HIPAA.[3] HHS has taken the position that only providers who actually use the standard format are covered by the

privacy regulation.[4] Currently, October 2002 is the deadline for compliance by most covered entities with the requirement for adopting the standard format, unless they meet the requirements for a one-year delay.[5]

B. What is Covered?

§ 160.103; § 164.501 and § 164.514(a) and (e))

"Protected Health Information"

Generally, the privacy regulation covers "protected health information" in any form that is created or received by a covered entity. There are a number of elements that must be satisfied before health information is protected by the regulation. First, it must be "health information" as defined in the regulation. Second, the health information must be individually identifiable. Finally, it must be created or received by a covered entity.

1. Health information

"Health information" is broadly defined as meaning 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 reasonably can be used to identify the individual. Health information that has been "de-identified" is not covered by the regulation. A covered entity may de-identify health information by removing specific identifiers (including, but not limited to, name, social security number, medical record number, and address). Alternatively, a covered entity may treat information as de-identified if a qualified statistician, using accepted principles, determines that the risk is very small that the individual could be identified.

- **Limited data set**[6] – A covered entity may also create a "limited data set" that, while not fully de-identified, has many direct identifiers (such as name, street address, telephone number, social security number) removed. A limited data set may be used or disclosed without an individual's authorization for certain purposes where a covered entity would be required to obtain the individual's authorization or meet other restrictions if it were using or disclosing fully identifiable information. (For a discussion of the conditions under which a limited data set can be used see "Treatment, Payment and Health Care Operations," "Public Health," and "Research" below.)

3. Created or received by a covered entity

Health information that is "created or received" by a covered entity is protected under the regulation. Any health information that a patient would divulge to his or her doctor would be covered. In contrast, health information that is created or received by others is

not covered. For example, if an individual fills out a health assessment survey as part of donating blood to the Red Cross, that information would not be protected because the Red Cross is not a covered entity.

If health information meets these criteria, it is considered "protected health information" and is covered by the regulation regardless of the media or form in which it is maintained or transmitted. This means that oral, written, and electronic information is protected.

The regulation protects the health information of both living and deceased individuals.

Note that while information maintained by many educational institutions may appear to meet these criteria, it is expressly excluded from the regulation.[7] In addition, HHS has clarified that employment records held by a covered entity in its capacity as an employer are excluded from the definition of protected health information. Individually identifiable health information created, received, or maintained by a covered entity in its health care capacity is still protected health information.[8]

C. Who May Exercise Privacy Rights

§ 164.501 and § 164.502(g)

For the most part, the rights afforded by the privacy regulation are exercised by the "individual," that 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 associated with the individual's health information. Personal representatives can include parents, guardians, executors of estates, and others. The rules for personal representatives vary depending on whom they represent.

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 must be treated as the personal representative of that individual. This includes court-appointed guardians and persons with power of attorney. The authority of a personal representative under this rule is 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.

Minors

Generally, a parent is considered to be the personal representative of an unemancipated minor,[9] and is deemed to have the rights associated with the minor's health information (such as the right to authorize a disclosure or to request access to health information). Under this general rule, in most cases a minor would *not* have the rights associated with his or her own medical information.

In certain circumstances an unemancipated minor *does* have rights associated with his or her health information. The regulation gives a minor rights with respect to health information that is related to treatment where:

- A minor is authorized by law to consent to treatment and has consented to care (with or without the consent of the parent);
- A minor may lawfully obtain care without parental consent and the minor, a court, or someone else authorized by law consents; or
- A parent has assented to an agreement of confidentiality between a provider and a minor.

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 is more complicated, and is largely governed by state law. The regulation 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 regulation 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.[10]

It is important to note that laws that govern when a minor may consent to treatment without parental involvement are not affected by the privacy regulation. State parental notification laws are also not affected by this regulation.

Victims of domestic violence, abuse, or neglect

A covered entity may elect not to treat a person as 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, or treating such person as the personal representative could endanger the individual, *and* the covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

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.

III. Patient Access

A. Right to Inspect and Copy

§ 164.524

The regulation establishes a new federal legal right for individuals to see and obtain a copy of their own protected health information in a designated record set[11] for as long as the information is maintained. It also establishes deadlines for covered entities to respond to requests for access and creates procedures for reviewing denials of those requests.

Provision of access

In general, the covered entity must allow the individual to inspect or obtain a copy of the protected health information in the form or format requested by the individual no later than 30 days after receiving the request (60 days if the information is not maintained or accessible to the covered entity on-site). The deadline may be extended 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.

The covered entity can provide the individual with an explanation or summary of the requested protected health information, if the individual agrees in advance to the arrangement and the fees imposed. The covered entity can impose "reasonable," cost-based fees for providing the individual a copy, explanation, 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.

Denial of access

A covered entity *may* deny an individual access to all or part of his or her protected health information *without* providing the individual an opportunity for review of that denial in the following circumstances:

- Psychotherapy notes;
- Information compiled in anticipation of or for use in a civil, criminal, or administrative action or proceeding;
- Protected health information maintained by a covered entity that is subject to the Clinical Laboratory Improvements Amendments (CLIA) or exempt from CLIA regulations;

- Information requested by an inmate, if providing a copy to the inmate would jeopardize the health, safety, security, custody or rehabilitation of the inmate or other inmates, or the safety of any officer, employee or other person at the correctional institution;

- Research that includes treatment – access may be suspended until completion of the project, provided that the individual was informed that he or she would be denied access until the research is completed and he or she agreed to the denial of access;

- 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.

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 if:

- 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 (except other health care providers) 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 within 30 days. 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 information on how the individual can file a complaint to the covered entity or to the Secretary of HHS.

Process for review of denial of access

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.

B. Right to Amend

§ 164.526

The regulation gives individuals the right to amend or supplement their own protected health information. For example, an individual who disagrees with a medical opinion could submit a second opinion to be included in the medical record. The individual has this right for as long as the covered entity maintains the information. 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 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.

Accepting requests for amendment

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 provide the amendment to both entities identified by the individual and other entities known to have received the erroneous information.

Denial of request for amendment

A covered entity *may* deny an individual's request for amendment if the entity determines that the information or record:

- Was not created by the covered entity, unless the originator of the protected health information is no longer available to make the amendment;
- Is not a part of the designated record set;
- Would not be available for inspection (see summary of right of access above); or
- Is accurate and complete.

If the covered entity denies an individual's request, it must give the individual a timely, written denial, which includes (1) the basis for the denial, (2) the individual's right to submit a written statement disagreeing with the denial and how to exercise that right, (3) 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 (4) a description of how the individual can file a complaint with the covered entity or the Secretary of HHS.

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.

IV. General Rules for Use and Disclosure

The regulation imposes restrictions on when and how covered entities may use and disclose protected health information. This section discusses the rules that are *generally* applicable. The regulation also establishes many detailed rules that must be followed when protected health information is used or disclosed for a specific purpose. These requirements are discussed below in "Specific Rules for Use and Disclosure."

A. "Use" and "Disclosure" Defined

§ 164.501

The regulation governs the "uses" and "disclosures" of protected health information. It is important to note the distinction between the terms since different rules may apply depending on whether information is being used or disclosed.

Use

Protected health information is *used* when it is shared, examined, utilized, applied or analyzed *within* a covered entity that maintains the information.

Disclosure

Protected health information is *disclosed* when it is released, transferred, has been given access to, or otherwise divulged *outside* the entity holding the information.

B. Permitted Uses and Disclosures—Overview

§ 164.502(a)

In the most general sense, the regulation prohibits a covered entity from using or disclosing protected health information except as expressly permitted or required by the regulation. For some purposes (treatment, payment and health care operations), the regulation permits a covered entity to use and disclose protected health information without the individual's permission and with only a few restrictions. In other circumstances (e.g., disclosures to family members), the regulation requires the covered entity to give the individual the opportunity to object to the disclosure. The regulation permits the use and disclosure of protected health information without the individual's permission, but subject to specific conditions, for many purposes that are not central to the treatment of the individual. For uses and disclosures that are not permitted by the regulation, a covered entity must obtain the patient's written authorization. These different circumstances are discussed separately below.

C. Permissive Not Mandatory

§ 164.502(a) and (b)

Under the privacy regulation, a covered entity is *required* to disclose protected health information only to the individual who is the subject of the information and to HHS for

enforcement of the regulation. The vast preponderance of the regulation addresses *permissive* uses and disclosures. In other words, in most circumstances, a covered entity can choose not to disclose information. HHS expects covered entities to rely on their professional ethics and use their own best judgments in deciding when they will permit the use and disclosure of protected health information.

D. Minimum Necessary

§ 164.502(b) and § 164.514(d)

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. There are a number of circumstances in which the minimum necessary standard does *not* apply. Disclosures to or requests by a health care provider for treatment purposes are not subject to the minimum necessary standard. Neither does the standard apply to: disclosures made to individuals pursuant to their request; those made to the Secretary for overseeing compliance of the privacy regulation; any uses or disclosures for which the covered entity has received an authorization; or uses or disclosures that are required by law.

In most cases, covered entities are not required to make a minimum necessary determination for each separate use and disclosure. Rather, they are required to implement policies and procedures to ensure that the minimum necessary standard is followed. Such policies would include identifying persons or categories of persons within an organization who need specific types of information and limiting those persons' access to only the information that they actually need.

General policies and procedures are not sufficient for disclosures that are *not* made on a routine, recurring basis. These disclosures must be reviewed on an individual basis to determine the minimum amount of protected health information necessary to disclose.

In certain circumstances, a covered entity may *presume* that a disclosure request meets the minimum necessary standard. For instance, a covered entity may rely on a disclosure request from another covered entity.

Using, disclosing, or requesting the entire medical record is not permitted except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the specified purpose.

E. Incidental Uses and Disclosures

§ 164.502(a)

Incidental uses or disclosures of protected health information that occur as a result of a use or disclosure permitted by the privacy regulation are not considered violations of the rule, provided that the covered entity has met the reasonable safeguards and minimum necessary

requirements. Examples of such incidental uses or disclosures include using sign-in sheets in waiting rooms, maintaining bedside patient charts, and engaging in confidential conversations that are overheard by others (despite reasonable measures to prevent such disclosures).

F. Business Associates

§ 160.103; § 164.502(e); § 164.504(e) and § 164.532(d) & (e)

Health plans and providers routinely hire other companies and consultants to perform a wide variety of functions for them. Health plans and providers, for example, may work with outside attorneys, bill collectors, computer specialists, or accreditation organizations. All of these entities need access to some patient information. But these persons are not directly subject to the privacy regulation. To allow information to be shared with these "business associates" and to protect the information that is disclosed to them, the regulation establishes specific conditions on when and how covered entities may share information with these entities. A "business associate" is a person 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

- Provides legal, actuarial, accounting consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity.

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.[12] (See later discussion of "Organized Health Care Arrangement" for more information.) Furthermore, the rule is not intended to cover anyone who merely acts as a conduit for protected health information, such as the U.S. Postal Service.

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, this safeguard will take the form of 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.[13] 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 a function.

Covered entities (except small health plans) have up to an additional year (April 14, 2004) to change written contracts to come into compliance with the business associate requirements if

those non-compliant contracts are entered into prior to October 15, 2002, and are not renewed prior to April 14, 2003. (Small health plans have until April 14, 2004 to comply with all of the regulation's requirements.) The regulation includes sample business associate contract provisions.

G. Authorization

§ 164.502(a) and § 164.508

There are two types of permission that are used to permit a covered entity to use or disclose protected health information: consent and authorization. A general "consent" is permitted but *not required* for use or disclosure of information for treatment, payment, and health care operations. ("Consent" is fully discussed in "Treatment, Payment, and Health Care Operations" below.) A more specific written "authorization" is required in certain circumstances. For instance, prior authorization must be obtained for most disclosures of psychotherapy notes. (See the discussion of "Psychotherapy Notes" under "Treatment, Payment and Health Care Operations," below.) An authorization is also specifically required to disclose health information for "marketing". Finally, an authorization is required for uses and disclosures that are not otherwise required or permitted by the privacy regulation.[14]

The regulation includes detailed requirements for the authorization form. All authorization forms must contain certain core elements, whether the request for disclosure is made by an individual or a covered entity. Among other things, a valid authorization must include the following:

- A specific description of the information to be used or disclosed and the purposes of the use or disclosure;
- The identity of the person or class of persons authorized to make the requested use or disclosure;
- The identity of the person or class of persons to whom the covered entity may make the requested use or disclosure;
- A statement of the person's right to revoke the authorization; and
- The signature and date of the authorization.

An individual who initiates an authorization is not required to reveal the purpose of his or her request. HHS has indicated that an authorization form may be signed with an electronic signature once the agency adopts electronic signature standards.

Most authorizations may not be combined with any other document to create a compound authorization, with a few specified exceptions such as using a single combined form to obtain

informed consent for participation in a research project and authorization to use or disclose protected health information for such research.

Revocation of authorization

An individual may revoke an authorization at any time. The revocation must be in writing and is not effective to the extent a covered entity has taken action in reliance on the authorization. Neither is it effective in certain circumstances where an insurer has the right by law to contest a claim under a policy or the policy itself.

Conditioning of authorization

Generally, a covered health care provider may not condition the provision of treatment on the individual's signing an authorization. A provider may, however, condition research-related treatment on the provision of an authorization or consent.

A health plan generally may condition enrollment in the health plan, eligibility for benefits, or the payment of a claim for specified benefits on the provision of an authorization related to such purposes. However, the health plan may not condition enrollment, eligibility or payment on the provision of an authorization for the use or disclosure of psychotherapy notes.

V. Specific Rules for Use and Disclosure

The regulation establishes different rules for different activities. In many cases, covered entities may use or disclose protected health information without patient authorization. Because the restrictions vary depending on the intended purposes, we have discussed the various purposes separately.

A. Treatment, Payment, and Health Care Operations

§ 164.501; § 164.506; § 164.520(c) and § 164.522

The regulation establishes standards under which covered entities may use and disclose health information for what are often considered the "core" health care purposes of treatment, payment, and health care operations. In the regulation, these purposes are broadly defined.

Treatment

"Treatment" means the provision, coordination, or management of health care, including consultations and referrals between health care providers. The term treatment is not limited to treatment of the specific individual who is the subject of the record; it is intended to encompass treatment of any and all individuals.[15]

Payment

"Payment" includes, but is not limited to, efforts to obtain premiums or reimbursement; determine eligibility; billing; claims management; review of health care for determining whether it is "medically necessary"; and utilization review.

Health care operations

"Health care operations" includes quality assessment and improvement activities; case management and care coordination; reviewing the competence or qualifications of health care professionals; underwriting; arranging for legal services; business planning; customer services; resolution of internal grievances; creating de-identified information; fundraising; and other activities.

General rule for use and disclosure

A covered entity may use and disclose an individual's protected health information for its own treatment, payment, or health care operations without obtaining the individual's permission (authorization or consent). In addition, a covered entity may disclose, without the individual's permission, protected health information for: the treatment or payment activities of a health care provider; the payment activities of another covered entity; and for certain health care operations of another covered entity, if each entity has or had a relationship with the individual who is the subject of the protected health information and the requested information pertains to that relationship.

In lieu of obtaining an individual's permission, direct treatment providers must make a good faith effort to obtain the individual's written acknowledgment of receipt of the entity's notice of privacy practices. (See "Administrative Requirements of Covered Entities" below for discussion of notice) This acknowledgment requirement does not apply to health plans, health care clearinghouses, providers that have an "indirect treatment relationship" with an individual (*e.g.*, a radiologist in a hospital setting) or in emergency situations.[16]

Consent[17]

A covered entity *may*, at its discretion, obtain the individual's consent to use or disclose protected health information for treatment, payment or health care operations. Covered entities that choose to obtain a patient's consent for these purposes have complete discretion in designing their consent form and process. The regulation does not define the term "consent" and does not specify any requirements for the content of consent forms.

Right to request restrictions

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. For example, an individual may request that a particular medical procedure be kept confidential and not shared with other providers. 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.

Psychotherapy notes

Psychotherapy notes are afforded special treatment and heightened protection.[18] Psychotherapy notes are limited to those notes that are recorded by a mental health professional documenting or analyzing the contents of conversation during counseling sessions and which are separated from the rest of the individual's medical record. An authorization is required for all uses and disclosures of psychotherapy notes except those listed in the regulation. For example, the originator of the psychotherapy notes may use them for treatment purposes; a covered entity may use or disclose them for its own training programs; and a covered entity may use or disclose them to defend itself in a legal action brought by the individual.

An authorization for use or disclosure of psychotherapy notes must meet the requirements discussed above in "General Rules, Authorization." The regulation specifically states that a health plan **may not condition** enrollment or the provision of benefits on the individual's authorization for the release of psychotherapy notes.

Limited data set

A covered entity may create and share a "limited data set" that it may use or disclose for health care operations without individual authorization. A limited data set, while not considered de-identified information, has the following direct identifiers removed: name, street address, account numbers and biometric identifiers; social security number; telephone and fax number; full face photo; and a few others. Because HHS perceives that there is a low

risk that an individual will be identified when a limited data set is utilized, the agency permits covered entities to use or disclose this information for health care operations. For instance a hospital can share a limited data set with a state hospital association in order for it to aggregate and analyze data from many hospitals for the purpose of quality improvement. HHS intends this provision to address, among other things, a state hospital association's ability to disseminate information that it has collected from various hospitals and aggregated and analyzed on their behalf.[19]

The regulation 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 would agree 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 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 violates a data use agreement, it is in noncompliance with the regulation. If the data recipient is not a covered entity, HHS cannot take enforcement activity directly against it.

B. Facility Directories

§ 164.510(a)

Many entities – such as hospitals – maintain a public directory of individuals at their facility. Under the regulation, a covered entity may use or disclose protected health information for facility directories without the written authorization of the individual provided that certain criteria are met. The entity must inform the individual *in advance* of the use or disclosure and provide him or her with an opportunity to agree or object (opt out). These communications can be oral. The information that may be used and disclosed for facility directories is limited to the individual's name and his or her location in the facility, general condition and religious affiliation. Under this provision, for example, florists would be able to deliver flowers to a patient in a hospital. The covered entity may disclose facility directory information to persons who ask for the individual by name. Additionally, directory information (including religious affiliation) may be disclosed to members of the clergy.

C. Those Involved in Providing Care (Next of Kin)

§ 164.510(b) and § 165.522

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 opt out; or

reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object. These agreements can be oral.

If an individual objects, the covered entity is prohibited from sharing health information with the patient's friends or relatives. When the individual is not present, the covered entity may use its best professional judgment and experience with common practice in deciding whether a disclosure is appropriate. A pharmacist, for example, generally may allow a person to act on behalf of the individual to pick up a prescription.

Right to request restrictions

In addition to the above right to opt out, through which an individual can totally prohibit disclosures to friends and relatives, an individual also has the right to request limitations on the relevant health information that he or she has agreed to release. The individual can request that the covered entity share only a *limited* amount or type of information with friends or relatives.

For example, a provider may believe that a patient's HIV status is directly relevant to providing care for his pneumonia. The patient may agree to have the fact that he has pneumonia disclosed to his mother (who is taking care of him), but may request that the provider not disclose that the patient is HIV positive. The covered entity does not have to agree to this requested restriction.[20] However, if the covered entity does enter into an agreement to disclose only select information, it must abide by that agreement, except in emergency circumstances.

D. Marketing

§ 164.501 and §164.508(a)(3)

The regulation requires a covered entity to obtain an individual's prior written authorization to use or disclose protected health information for "marketing." The key to understanding how this authorization requirement operates is to understand the limited scope of the definition of marketing. It is equally important to be familiar with the activities that are expressly excluded from the definition.

The regulation initially defines "marketing" as a communication about a product or service that encourages the recipient to purchase or use the product or service. The regulation then expressly excludes various types of communications from this definition: those that describe a health-related product or service that is provided by the covered entity; those that describe the entities participating in a provider or plan network; those that describe health-related products or services available to health plan enrollees that add value to (and are not part of) the plan's benefits; those for treatment of the individual; those made for case management or care coordination; and those made to direct or recommend alternate therapies, providers, or settings of care. In essence, these provisions only require an individual's prior authorization for communications that encourage an individual to use or purchase a service or product that

is *not* health related. Communications that are related to health care are *not* marketing under the regulation so they do not require prior written authorization.

Under these provisions, many common practices are permitted without obtaining a patient's authorization. For example, a physician who recommends a brand name medication to a patient would not be considered to be engaged in marketing. However, these provisions also exclude from "marketing" many communications that are considerably more controversial. For example, communications from pharmacies, paid for by drug manufacturers, in which the pharmacy recommends that the individual switch his or her medication to the drug company's product would not be considered marketing under the regulation, and thus would not require prior authorization.[21] It is notable that the regulation does not specify any means for opting out of such communications.

Furthermore, a covered entity does not need patient authorization if it uses or discloses protected health information for marketing that occurs face to face or if the marketing communication involves a promotional gift of nominal value.

The regulation does clarify, however, that a covered entity cannot sell lists of patients or enrollees to third parties for the marketing activities of the third party without the individual's authorization.

Where an authorization is required, the authorization must disclose whether the marketing involves direct or indirect remuneration to the covered entity from a third party.

For any of the communications permitted by this part of the regulation, a covered entity is permitted to disclose protected health information to a business associate to assist with the communication.

E. Fundraising

§ 164.501; § 164.514(f) and § 164.522

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 it meets certain criteria:

- 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.

F. Averting a Serious Threat to Health or Safety
§ 164.512(j)

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 it is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Any disclosure must be to a person reasonably able to prevent or lessen the threat, which could include the target of the threat. Other conditions apply to such disclosures.

G. Health Oversight Activities
§ 164.512(d)

Disclosures may be made to health oversight agencies for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; and other activities. The regulation attempts to clarify that this provision does not encompass investigations of individuals that are not related to the receipt of health care or claims for public benefits related to health care.[22]

H. Judicial and Administrative Proceedings
§ 164.512(e)

The regulation 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 that 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. Alternatively, the party seeking the information may obtain a protective order. The rule sets out specific elements that must be met to fulfill the "satisfactory assurance" criteria.

I. Law Enforcement

§ 164.512(f)

A covered entity may disclose protected health information to law enforcement officials as required by law or pursuant to:

- A court order, a court-ordered warrant, or a subpoena or summons issued by a judicial officer;
- A grand jury subpoena; *or*
- An administrative request, such as an administrative summons or a civil investigative demand, that meets specific standards.

Additionally, the regulation does not require any consent or authorization for the disclosure of certain categories of protected health information to law enforcement officials for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. Covered entities may also disclose protected health information about a crime victim to law enforcement officials. Other disclosures are also permitted.

J. Public Health Activities

§ 164.512(b) and § 164.514(e)

A covered entity may disclose protected health information for "public health purposes" to certain specified recipients including: public health authorities (such as the Centers for Disease Control and Prevention, Occupational Safety and Health Administration, and state public health agencies); persons subject to the jurisdiction of the Food and Drug Administration for public health purposes related to the quality, safety or effectiveness of FDA-regulated products or activities; and to persons exposed to a communicable disease (if otherwise authorized by law to notify such a person). Additionally, in certain circumstances, a health care provider may disclose to an employer protected health information about an individual who is a member of that employer's workforce**.**

A covered entity is also permitted to use or disclose a limited data set (protected health information from which many direct identifiers, such as name and social security number have been removed) for public health purposes. For example, a covered entity may disclose a limited data set to a private disease registry for a public health purpose without the individual's authorization. In contrast, the disclosure of fully identifiable information to such a registry would require authorization. (For the full discussion of "limited data sets" see "Individually Identifiable Information" (where the term is defined) and "Treatment, Payment, and Health Care Operations, Limited data set.")

K. Required by Law

§ 164.512(a)

A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law.

L. Research

§ 164.512(i) and § 164.514(e)

The regulation allows covered entities to disclose protected health information to researchers *without* patient authorization if an Institutional Review Board (IRB) or "privacy board" approves a waiver or alteration of authorization. Generally, the regulation seeks to extend the waiver of informed consent provisions of existing regulations – known as the "Common Rule" – that apply to federally-funded research to cover all research, regardless of the source of funding. If the researcher provides treatment as part of the research study and submits insurance claims electronically for payment of the care provided, the researcher will be treated as a covered health care provider, and must comply with all relevant sections of the regulation.

IRBs and privacy boards

This regulation allows information to be disclosed to researchers if the research has been approved by an IRB (as stipulated in the Common Rule) or by a newly formed "privacy board." The regulation is specific in the composition of a privacy board. For example, it requires that at least one member not be associated with the entity sponsoring the research.

Review criteria

The regulation requires research to meet three criteria for the waiver or alteration of authorization:

(1) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:

(a) An adequate plan to protect the identifiers from improper use and disclosure;

(b) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(c) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by the regulation;

(2) The research could not practicably be conducted without the waiver or alteration; and

(3) The research could not practicably be conducted without access to and use of the protected health information.

The regulation allows the waiver of authorization to be approved by normal review procedures, or by expedited review if the research is of "minimal risk" to the subjects. Expedited review allows the chair of the IRB or privacy board or a designate to approve the waiver alone, rather than by a majority vote.

Additional disclosures to researchers

The regulation allows information to be disclosed to researchers without authorization in two additional circumstances: the information is necessary to prepare a research protocol (that presumably would later be presented to an IRB) or some other activity in preparation for research; or the research uses decedent information. In both cases, certain conditions must be met.

Covered entities may also use or disclose a limited data set to researchers without authorization or a waiver of authorization from an IRB or privacy board. (See "Limited data set" under "Treatment, Payment, and Health Care Operations," Section V (A) above for a full discussion of the conditions under which limited data sets may be used and disclosed.)

M. Victims of Abuse, Neglect, or Domestic Violence

§ 164.512(c)

A covered entity may disclose information about 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. 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.

N. Workers' Compensation

§ 164.512(l)

A covered entity may disclose protected health information as authorized by laws relating to workers' compensation or other similar programs. Again, workers' compensation carriers are not considered health plans in the regulation, and are therefore not covered by the regulation.

VI. Administrative Requirements of Covered Entities

A. Notice

§ 164.500 and § 164.520

The regulation requires a covered entity to provide individuals with a written notice describing the entity's privacy practices. Health plans are required to give notice at enrollment and to notify individuals every three years that the privacy practices notice is available. Providers that have a direct treatment relationship with an individual are only required to give notice at the date of the first service delivery; and except in emergency circumstances, must make a good faith effort to obtain a written acknowledgment from the individual of receipt of the notice. Providers must also have notice posted on the premises. Both plans and providers have special notice requirements if their privacy practices change. (See below for further discussion.) Clearinghouses acting as business associates of another covered entity are not required to give notice to patients.

The notice must include:

- A description of an 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 of information that are permitted, including those that are permitted or required without the individual's written authorization;
- How an individual can file complaints with the covered entity and the Secretary of HHS;
- How the covered entity will provide the individual with a revised notice if the notice is changed;
- A contact person for additional information; and
- The date on which the notice is in effect.

The regulation imposes requirements on when and how the covered entity's privacy policy and procedures can be revised. Notice must be given to individuals before any new policy is implemented. The revised policy does not apply to information previously obtained unless the covered entity follows certain procedures. Specifically, 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 was in effect. Any change would apply only to information created or received after the effective date of the revised notice.

The notice provisions of the regulation also include specific requirements regarding electronic notice and joint notices by separate covered entities.

B. Safeguards
§ 164.530(c)

The covered entity must have appropriate administrative, technical, and physical safeguards in place to protect the privacy of protected health information, and reasonably safeguard such information from intentional or unintentional use or disclosure.[23]

C. Training
§ 164.530(b)

A covered entity must train all members of its workforce on the policies and procedures regarding protected health information required by the regulation no later than the its compliance date with the regulation and within a reasonable period of time for each new member of its workforce.

D. Privacy Officer
§ 164.530(a)

The regulation requires a covered entity to designate a privacy official for the development and implementation of its policies and procedures.

E. Accounting for Disclosures
§ 164.528

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 that the individual requests the accounting, including disclosures to or by business associates. 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.*, using or sharing health information *within* a covered entity. For example, an individual would not have a right to a list of all hospital employees who have had access to his or her health information. 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 statement of the purpose of the disclosure.

The covered entity must provide the individual with the accounting of disclosures no later than 60 days after it receives the request. The deadline may be extended up to 30 days. The first accounting provided to an individual in any 12-month period is free.

The regulation specifically includes provisions that apply when a covered entity discloses the protected health information of 50 or more people in connection with a research project.[24] These provisions allow the entity to include general information about such research-related disclosures whether or not the protected health information of the individual who requested the accounting actually was disclosed.

There are a few exceptions to the individual's right to receive an accounting of disclosures, and they are specified in the regulation. 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. In effect, this means that patients do not have a right to know the names of *everyone* who has seen their records. They will not know who has seen their records in the course of providing or paying for care.

The regulation also exempts from the accounting requirement disclosures made pursuant to an authorization and disclosures that are part of a limited data set. The covered entity must also temporarily suspend the individual's right for 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.

VII. Special Rules for Certain Types of Entities

Some organizations do not fit neatly within the rules for covered entities. They might have only a small component that performs covered health care functions. Or the organization might perform multiple covered functions that are subject to differing rules. Group health plans have been of particular concern because of their relationship with the employers who sponsor the plans. The regulation sets out specific rules that apply to these different types of covered entities.

A. Hybrid Entity

§ 164.504(a)-(c)

The term "hybrid entity" is used to describe an organization that has a component that is a health plan, health care clearinghouse, or a covered health care provider, and whose business activities include both covered and non-covered functions. The hybrid entity status is optional: The regulation does not impose this status on any covered entity. In order to be considered a hybrid entity the covered entity must designate the segments of its business that comprise the health care components. A covered entity may designate a part of its business as a health care component only to the extent that it either: 1) performs covered functions; or 2) conducts activities that would make it a business associate of the segment that performs covered functions if the two components were separate legal entities.

The entire hybrid entity is considered to be the covered entity under the regulation, and it has the overall responsibility for ensuring compliance with the regulation and for implementing safeguards to ensure against the improper use or disclosure of information within the organization, such as establishing firewalls. For most practical purposes, the regulation *treats* only the health care component as the "covered entity" and the remaining organization as if it were a separate uncovered entity.

The health care component is generally prohibited from sharing protected health information with the larger organization unless the disclosure has been authorized by the individual or is otherwise permitted by the regulation. For example, a manufacturing firm that has a health clinic might be considered to be a hybrid entity. The health clinic would be the health care component and would be prohibited from sharing protected health information with other departments in the firm.

B. Affiliated Covered Entity

§ 164.504(d)

Legally distinct covered entities that are under common ownership or control may designate themselves as a single covered entity for purposes of the privacy regulation.[25] Such a designation allows all of the affiliates to use and share protected health information as if they were a single covered entity. For example, a corporation with hospitals in twenty states can

designate itself as a single covered entity. As such, they can merge patient information for all permitted uses and disclosures.

C. Multiple Covered Function Entity
§ 164.504(g)

A covered entity may (as a single legal entity, affiliated entity, or other arrangement) combine the functions of health care providers, health plans, and health care clearinghouses. For example, integrated health plans and health care delivery systems may function as both health plans and health care providers. For purposes of using and disclosing protected health information, each function is essentially treated as a separate covered entity. Thus, a covered entity may not use or disclose the protected health information of an individual who receives health *care* from the organization for health *plan* purposes (unless, of course, that individual is also a member of the health plan).

D. Group Health Plan (Restrictions on Disclosures to Employers)
§ 164.504(f)

"Group health plans" are covered entities under the regulation. These plans present a particular set of problems due to their interrelationship with employers and other sponsors, which, although *not* covered entities, may use individual health information to carry out plan functions. For instance, an employer may carry out administrative functions on behalf of the group health plan that it sponsors. There is a concern, however, that health information shared with the employer may be used inappropriately in employment-related decisions. To reconcile these varying needs, the regulation permits a group health plan to disclose protected health information to a plan sponsor without a business associate contract for plan administration purposes, but *prohibits* disclosure for employment-related actions.

The regulation carries out this scheme by requiring that a group health plan's documents be amended so that they limit the uses and disclosures of health information by the plan sponsor to those consistent with the privacy regulation.[26] Specifically, in order for a group health plan to disclose protected health information to a plan sponsor, the plan documents must (1) describe the permitted uses and disclosures of protected health information by the sponsor (consistent with the regulation); and (2) provide that disclosure is permitted only upon receipt of a certification from the plan sponsor. The certification must provide that the plan sponsor agrees that it *will not use* or disclose the information for employment-related actions and decisions. Furthermore, the employer must agree to provide adequate firewalls to restrict access to the information only to employees identified as needing access to perform functions on behalf of the group health plan. The sponsor must also certify that it has agreed to a number of other conditions.

E. Organized Health Care Arrangement

§ 164.501 and § 164.520

Health care is often delivered through arrangements that involve clinical or operational integration among legally separate entities in which it is often necessary to share protected health information. The regulation recognizes a number of general arrangements as "organized health care arrangements." These include a clinically integrated care setting in which individuals typically receive health care from more than one health care provider. An example of this arrangement is the hospital setting where a provider has staff privileges. "Organized health care arrangement" also includes the situation in which multiple covered entities hold themselves out to the public as participating in a joint arrangement. For example, an independent practice association formed by a large number of physicians would come within this description. There are also arrangements involving group health plans that are recognized as organized health care arrangements.

Covered entities that participate in an organized health care arrangement may issue a **joint notice of privacy practices**. In addition to the general requirements for such notices, a joint notice of privacy practices must describe the covered entities (or class of entities) to which the joint notice applies, as well as the delivery sites covered. If applicable, it must also state that the covered entities participating in the organized health care arrangement will share protected health information with each other as necessary to carry out treatment, payment, and health care operations.

VIII. Enforcement and Compliance

The general approach that the regulation takes to compliance and enforcement is, whenever possible, to work cooperatively with covered entities. Additionally, pending the availability of staff and other resources, the Secretary of HHS is committed to assisting covered entities in complying with the regulation through technical assistance.

Any person who believes a covered entity is not complying with the applicable requirements of the regulation may file a complaint with the Secretary. A person is defined broadly to include not just human beings, but also any type of association, group, or organization.

A. Complaints

§ 160.306 and § 160.312

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 that violated the regulation; and

3. The complaint must be filed within 180 days of when the complainant knew (or should have known) of the violation of the regulation. The Secretary has the authority to waive the time limit if there is a showing of good cause.

The Secretary also may prescribe additional procedures for the filing of complaints by publishing a notice in the *Federal Register*.

The Secretary is authorized to conduct an investigation of the complaint. This investigation may review relevant policies, procedures, and practices of the covered entity and the specific circumstances of the complaint.

After an investigation, the Secretary will notify the covered entity and the complainant of the outcome of the investigation. If there is a finding of noncompliance, the Secretary will, whenever possible, attempt to resolve the matter informally.

B. Compliance Reviews

§ 160.308; § 160.310 and § 160.312

The regulation authorizes the Secretary to conduct compliance reviews to determine whether covered entities are complying with the regulation. As with the investigation of a complaint, the Secretary will notify the covered entity of the outcome of the review. If a finding of

noncompliance is made, the Secretary will, whenever possible, attempt to resolve the matter informally.

The regulation 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, covered entities must permit the Secretary, 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 regulation. Under exigent circumstances, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary at any time without notice.

Protected health information that is obtained by the Secretary in connection with an investigation or compliance review will not be disclosed by the Secretary unless it is necessary for ascertaining or enforcing compliance with the regulation, or disclosure is otherwise required by law.

C. Penalties

HIPAA establishes civil and criminal penalties for violations of the regulation. There is a $100 civil penalty up to a maximum of $25,000 per year for each standard violated. Criminal penalties are imposed for certain wrongful disclosures of health information. It is a graduated penalty that may escalate to a maximum of $250,000 for particularly egregious offenses.

HIPAA does not create a federal right to sue for violations of the Act. However, because the new regulation creates a new "duty of care" with respect to health information, it is possible that violations may be the grounds of state tort actions.

IX. Preemption

§ 160.201; § 160.202; § 160.203; § 160.204 and § 160.205

The regulation establishes a uniform "floor" for protecting the privacy of protected health information. State laws that are contrary to the federal regulation and that are less protective are preempted.[27] Existing or future state laws related to the privacy of health information that are *more stringent* than the federal rule will remain in effect, even if they are contrary to the federal regulation.[28]

Generally, a state law is "more stringent" when it provides greater privacy protection for the individual who is the subject of the information. The regulation also explains when a law is more stringent in specified circumstances. For instance, a state law is more stringent when it prohibits or restricts a use or disclosure that would be permitted under the regulation. With respect to laws that govern patient access, a state law is "more stringent" when it provides individuals with greater access to their own information.

State laws that provide for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health investigations are not preempted by the federal privacy rule. Furthermore, state laws that require health plans to report or grant access to information for the purpose of audits, evaluation, or licensure will remain in effect even if they are less protective of individuals' privacy.

States and others also can request that the Secretary except a state law from preemption. An exception can only be granted if certain criteria are met. For instance, the Secretary may except state laws that he finds necessary to prevent fraud and abuse related to the provision of or payment of health care. Once a state law is excepted from preemption, that state law will remain in effect until there is a material change in either the state law or the analogous federal regulation such that the grounds for the exception no longer exists. Alternatively, the Secretary can revoke the exception.

Endnotes

[1] High-risk pools are designed to provide health insurance coverage for individuals who, due to health status or pre-existing conditions, cannot obtain insurance through the individual market or who can do so only at very high premiums.

[2] *See* 42 U.S.C. Sec. 1320d-2(a) for the full list of electronic transactions that will trigger coverage of the privacy regulation.

[3] Health care providers and health plans currently use many different formats to conduct administrative and financial health care transactions electronically. To reduce health care costs and administrative burdens on providers and plans, HIPAA requires HHS to adopt national standards for such transactions. "Standard format" is used throughout this report to refer to the national formats for electronic health care data interchange, which health plans, health care clearinghouses and certain health care providers will be required to comply with by October 2002. Under the Administrative Simplification Compliance Act, Pub. Law 107-105, a covered entity that cannot meet the October 2002 deadline may qualify for a one-year delay if it submits a compliance plan to HHS no later than October 16, 2002. For more information about the transaction standards, visit the HHS Administrative Simplification Web site at http://aspe.hhs.gov/admnsimp/bannertx.htm.

[4] Although the language of the statute and the regulation can be read to cover any provider who transmits health information in electronic format (whether it is in standard format or not), HHS has taken the public position that the rule will apply only to those providers who engage in transactions in standard format. *See* 65 Fed. Reg. 82476-7 (Dec. 28, 2000) and 64 Fed. Reg. 59937 (Nov. 3, 1999).

[5] A one-year delay in the deadline for complying with the transaction standards does not affect the compliance date of the privacy regulation. *See* 147 Congressional Record S13077 (daily ed. December 12, 2001) (statement of Senator Dorgan).

[6] It appears that HHS did not follow appropriate procedural requirements when it included the limited data set provisions in the modifications published on August 14, 2002, because in its March 2002 proposal, HHS did not propose specific language on this topic. This would appear to violate the public notice and comment requirements of the Administrative Procedures Act.

[7] *See* § 164.501.

[8] *See id.*

[9] An "unemancipated minor" is a person who is not yet legally an adult, but who may have some of the rights and privileges of an adult. Specific ages and other criteria for emancipation are defined in state law, *not* by the federal regulation.

[10] These same rules also apply to any other law that relates to a parent's right of access to (or a provider's ability to disclose to a parent) an unemacipated minor's health information.

[11] "Designated record set" is defined as a group of records maintained by or for a covered entity that is used to make decisions about individuals. It includes a health care provider's medical records and billing records, and a health plan's enrollment, payment, claims adjudication, and medical management record systems.

[12] If the hospital were to provide billing services for the doctor, a business associate relationship would arise with respect to those services since they are being performed on behalf of another covered entity.

[13] The contract must also provide that the business associate will:

- Report to the covered entity any known inappropriate use or disclosure;
- Ensure that any agents (such as a subcontractor) agrees to the same restrictions on the covered information;
- Make available protected health information in its possession for inspection, copying, and amendment;
- Incorporate any amendments forwarded by the covered entity;
- Make available information required to provide an accounting of disclosures;
- Make its relevant books relating to the uses and disclosures of protected health information available to the Secretary for compliance oversight; and
- Return or destroy all protected health information received from, or created or received on behalf of the covered entity at the termination of the contract, if feasible.

[14] The regulation provides for many circumstances in which no authorization is required for the use or disclosure of protected health information. In many cases special conditions must be met for these uses and disclosures. We discuss these requirements in "Specific Rules for Use and Disclosure."

[15] Information about any patient may be disclosed if a covered entity believes that it might help to treat *another* patient. In other words, disclosures related to "treatment" do not have to be related to the subject of the information. Many disclosures might be justified under this definition.

[16] An indirect treatment relationship exists where the provider delivers health care to the individual based on the orders of another provider and the services, products, diagnoses or results are typically provided through another provider. An indirect treatment relationship, for example, might exist between a patient and a lab technician, a radiologist in a hospital setting, or a provider consulting on a case with the treating physician.

[17] The December 28, 2000 privacy regulation included a requirement that direct treatment providers obtain an individual's written consent to use or disclose protected health information for treatment, payment or health care operations purposes. The August 2002 modifications remove this consent requirement from the regulation. For a discussion of the modifications, see 67 Fed. Reg. 53208-53214.

[18] Not all information held by therapists comes within the definition of "psychotherapy notes." Information related to medication prescription, counseling start and stop times, results of clinical tests, summary of diagnosis and prognosis, and similar matters are treated as regular health information and may be disclosed under the general rules governing treatment, payment, and health care operations.

[19] Although this intent is expressed in the preamble to the regulation, it is questionable whether the regulation as written accomplishes this goal. *See* 67 Fed. Reg. 14799 (March 27, 2002) and 67 Fed. Reg. 53234 (August 14, 2002).

[20] Of course, if the covered entity does not agree to limit the information disclosed, the individual retains the right to prohibit the disclosure of *any* information to a friend or family member. To follow up on our previous example, if the provider does not agree to restrict the disclosure of the patient's HIV status, the patient can decide that he does not want any health information released to his mother.

[21] This is because "recommend[ing] alternative treatments" is not considered to be "marketing" even where the provider is making the recommendation primarily due to financial incentives.

[22] President Clinton signed an executive order on December 20, 2000 that prohibits federal law enforcement officials from using health information obtained in the course of a health oversight investigation against an individual in an action unrelated to the oversight investigation. There are some exceptions to the general rule. The order is designed to ensure that where patients have disclosed criminal activity to their provider, that it cannot be used against them if it is discovered in an oversight investigation. In other words, the information law enforcement collects in the course of an oversight investigation should only be used for those purposes, and should not be further disclosed. Exec. Order No. 13,181, 65 Fed. Reg. 81,321 (2000).

[23] In addition, more detailed HIPAA-mandated security regulations are expected to be finalized. HHS, however, has not provided a target date for the release of the final regulations.

[24] *See* § 164.528(b)(4).

[25] Common control exists if an entity has the power (directly or indirectly) significantly to influence or direct the actions or policies of another entity. Common ownership exists if an entity possesses an ownership or equity interest of 5% or more in another entity. § 164.504(a).

[26] The group health plan may also disclose summary health information to the plan sponsor, if requested, for the purpose of obtaining premium bids for providing health insurance or for the purpose of modifying, amending or terminating the group plan. In addition, the regulation allows a group health plan, a health insurance issuer, or HMO acting for a group health plan to disclose to a plan sponsor information on whether the individual is enrolled in or has disenrolled from a plan offered by the sponsor without amending the plan documents.

[27] A law is "contrary to" the federal regulation when (1) a covered entity would find it impossible to comply with both the State and federal requirements; or (2) the provision of State law stands as an obstacle to the accomplishment and execution of the purposes and objectives of the federal rule.

[28] *See* Health Privacy Project, *The State of Health Privacy: An Uneven Terrain (A Comprehensive Survey of State Health Privacy Statutes),* August 1999, for analysis of major state health privacy laws. Updated summaries of state health privacy statutes are available at http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm.