

HIPAA PRIMER

April 14, 2003: Deadline for compliance with the Health Insurance Portability and Accountability Act (HIPAA) privacy rule

WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA), which was enacted as the result of a bill sponsored by Senators Nancy Kassebaum (R-KS) and Ted Kennedy (D-MA), is designed to protect Americans who were previously ill from losing their health insurance when they changed jobs or residences.

The law also focuses on streamlining the health care system by adopting consistent standards for transmitting uniform electronic health care claims. The transaction rule requires standard formatting of electronic transactions for certain specified financial and administrative purposes, such as health care claims or plan eligibility or coverage inquiries.

Because of a concern about privacy issues related to this streamlined system, the HIPAA legislation required adoption of standards for securing storage of information and for protecting an individual's privacy. The proposed security rule, which has not yet been released in final form, addresses a provider organization's physical infrastructure, such as access to offices, files and computers to assure secure and private communication and maintenance of confidential patient information. The privacy rule requires policies, procedures, training and business service agreements to control the access and use of patient information.

FEDERAL GOVERNMENT ENFORCEMENT AND PENALTIES

There are significant penalties for non-compliance. If a health care provider refuses to become informed or deliberately fails to take appropriate action, the consequences of failing to comply with HIPAA may include (from the least to the most severe):

- Administrative action taken by the HHS Office for Civil Rights.
- Civil Penalties of not more than \$100 for each violation with the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year not to exceed \$25,000.
- Fines of up to \$250,000, imprisonment for up to 10 years, or both for knowingly violating "wrongful disclosure of individually identifiable health information."

It is expected that an initial enforcement aim of the HHS Office for Civil Rights will be to work with the health care community to help providers understand and implement HIPAA.

HOW WILL HIPAA'S PRIVACY RULE AFFECT ANOKA COUNTY?

Federal regulators appear to have given little thought or direction to how the privacy rule impacts county programs or which county programs are health care components required to comply with HIPAA.

The Minnesota government data practices act already places a high priority on safeguarding private data. In general, the privacy rule will require the health care components of Anoka County to:

- Provide information to consumers about their privacy rights and how health information can be used.
- Adopt clear privacy procedures.
- Train employees so that they understand the privacy procedures.
- Designate an individual to be responsible for seeing that privacy procedures are adopted and followed.
- Secure consumer records.
- Account for certain disclosures of health information.

The privacy rule covers many different types of health care providers, ranging from large multi-hospital systems to individual solo practitioners. The administrative and procedural requirements were designed for scalable compliance, meaning that a provider takes reasonable steps to meet the requirements according to its size and type of activities.

PREEMPTION OF STATE LAW

The privacy rule serves as a minimum level of privacy protection. It only takes precedence over those

Minnesota laws that provide less privacy protection or that provide consumers with less access to and control over their own health information.

Minnesota laws that provide better protection from the consumer's vantage point are not pre-empted. In those situations, Minnesota law still needs to be followed. This approach is intended to provide better protection for consumers. It also means providers are expected to be aware of all state laws that pertain to the privacy of health care information and to decide in any situation whether to follow state law, HIPAA privacy rules, or both.

HIPAA does not preempt state law:

- When state law provides for the reporting of disease or injury, child abuse, births or deaths, or for the conduct of public health surveillance, investigation or intervention
- When state law requires a health plan to report, or to provide access to, information for the purpose of management and financial audits, program monitoring and evaluation or the licensure or certification of facilities or individuals
- When, at the request of a state governor, the Secretary of HHS determines that a particular provision of state law is necessary: To prevent fraud and abuse related to health care; To ensure appropriate regulation of insurance and health plans; For state reporting on health care delivery or costs; or For purposes of serving a compelling need related to public health, safety or welfare. This request involves a formal process that only may be conducted by the state.

The privacy rule preempts on a provision by provision basis, not law by law. In other words, if one provision of a state privacy law is preempted, another provision in the same law may not be.

THE PRIVACY RULE APPLIES TO HEALTH INFORMATION

Important definitions include:

- Health Information: Any information, whether oral or recorded in any form, created or used by health care professionals or health care entities.

Note: Some county employees who typically are not thought of as health care professionals will be for purposes of HIPAA because their services are paid for with medical assistance funds.

- Health Care: Care, services or supplies related to the health of an individual including but not limited to the following: preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and the sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
- Individually Identifiable Health Information: A subset of Health Information that either identifies the individual or that can be used to identify the individual.
- Protected Health Information (PHI): Individually Identifiable Health Information becomes Protected Health Information (PHI) when it is transmitted or maintained in any form or medium. More specifically, PHI is information that relates to the past, present or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and that identifies the individual or could reasonably be used to identify the individual.

Health information that does not identify an individual and provides no reasonable basis to believe that the information can be used to identify a person is not considered PHI.

Individually Identifiable Health Information in educational records that are covered by the Family and Educational Right and Privacy Act. (20 U.S.C. 1232g) are also excluded from the definition of PHI.

WHAT TRIGGERS APPLICATION OF PRIVACY RULE?

A health care provider transmits PHI in electronic form in connection with any of the following types of transactions: Health care claims; Health care payment and remittance advice; Coordination of benefits;

Health care claim status, enrollment or disenrollment in a health plan; Eligibility for a health plan; Health plan premium payments; Referral certification and authorization; First report of injury; or Health claims attachments.

The privacy rule applies whether the provider transmits directly or uses a billing service acting on behalf of the provider to transmit health information in electronic form. Once triggered, the privacy rule applies to all information, not just to information in electronic form.

The mode of electronic transmission includes: the Internet, extranets (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk or compact-disk media.

Because Anoka County uses electronic transactions to file medical assistance claims with DHS, Anoka County is a covered entity that must comply with HIPAA. Since Anoka County is not primarily a health care provider, it can qualify to be treated as a hybrid entity. In a hybrid entity, only health care components must comply. But, because health care is broadly defined, many social services programs will have to comply with HIPAA.

PERMITTED USES UNDER HIPAA

HIPAA permits PHI to be used for activities related to Treatment, Payment and Health Care Operations.

➤Treatment: The provision, coordination or management of health care and related services by one or more health providers. The treatment definition includes consultation between health care providers relating to a patient or the referral of a patient from one health care provider to another.

➤Payment: Payment refers to the activities one undertakes to obtain reimbursement for health care services that have been provided. These activities can include, among others: determinations for eligibility or coverage, billing, claims management, collection activities and utilization review.

➤Health Care Operations: Health care operations is a very broad category of activities ranging from quality assessment and utilization review to conducting or arranging for medical reviews, legal services and auditing functions, business planning and administrative services.

Permitted use is one area where Minnesota law will provide greater protection as a result of more stringent state laws. Even though HIPAA may permit routine use of PHI for Treatment, Payment, and Health Care Operations, Minnesota law may require the consumer authorize disclosure of PHI. In any situation in which informed consent was required before HIPAA, the consumer's authorization still will be needed in order to disclose PHI.

AUTHORIZATION FOR DISCLOSURE OF PHI

PHI may be disclosed with the authorization of the consumer or the consumer's legal representative (legal guardian).

Authorizations, which have been typically referred to in Minnesota as informed consent or releases, must meet certain requirements specified by the privacy rule. An authorization must contain the following:

- A specific definition of the information to be used or disclosed
- To whom the information is going to be disclosed
- The purpose of the disclosure
- An expiration date
- The right to revoke
- The right not to authorize the disclosure

MINIMUM NECESSARY DISCLOSURE

When PHI is disclosed or used, the privacy rule requires providers to share the minimum amount of information necessary to conduct the activity. A couple of important points to note:

➤ The privacy rule also applies to PHI available internally to employees so they can do their jobs (e.g., a billing clerk may have access to the minimum amount of information needed to perform the billing role that would not include clinical information).

➤ In a treatment context, the minimum necessary provision does not apply. As permitted by state law, providers are free to share information they wish with another provider for the purpose of providing treatment.

➤ Minimum necessary disclosure does not apply to requests for information that require authorization. This is because the information to be disclosed must be specifically described in the authorization itself.

USE AND DISCLOSURE

The privacy rule defines a use as the sharing, employment, application, utilization, examination or analysis of individually identifiable health information within an entity that maintains such information. The privacy rule defines a disclosure as the release, transfer, provision or access to, or divulging in any other manner of information outside the entity holding the information.

There are a number of circumstances in which the privacy rule permits providers to make certain disclosures without authorization. These may include providing information to:

- A public health authority as required under state law
- A health oversight agency
- A coroner or medical examiner
- The military or another entity for national security purposes
- An authority with responsibility to investigate child abuse and neglect
- An appropriate person to avert a serious threat to health or safety

DEALING WITH THE JUDICIAL SYSTEM AND ADMINISTRATIVE PROCEEDINGS

PHI can be disclosed without authorization or an opportunity for the consumer to object in response to a court order or an order from an administrative tribunal (e.g., the Social Security Administration).

According to the privacy rule, PHI also may be disclosed in response to a non-court-ordered subpoena, discovery request or other legal process not accompanied by a court order if satisfactory assurance is provided demonstrating that reasonable efforts have been made to ensure that the consumer has been given notice of the request or that reasonable efforts have been made to secure a qualified protective order. But Minnesota law is more stringent than this HIPAA provision.

PATIENTS RIGHTS AND RECORDS

Consumers in many states will now have greater access to their records and greater knowledge of how their records will be used than ever before. In Minnesota, state law already provided for access to health records.

Under HIPAA, consumers have the right to:

- Receive notice about the uses and disclosures of their PHI made without their authorization
- Authorize disclosure of their PHI
- Access their records for inspection and amendment
- Receive an accounting of how their PHI was shared without their authorization for purposes other than treatment, payment or health care operations

Under HIPAA, a consumer does not have the right to access psychotherapy notes, which are defined as notes kept separately only for use by the psychotherapist. But the Minnesota government data practices act does not provide for this category of data to be withheld from a data subject.

AMENDMENT OF RECORDS

Right of amendment refers to the ability of a consumer to request a change in their PHI if they feel the PHI is incorrect.

A provider can deny requests for record amendments if not the originator of the information or if the information is accurate and complete. The Minnesota government data practices act also has a procedure to challenge the accuracy and completeness of data on an individual.

ACCOUNTING FOR DISCLOSURES

Right of accounting refers to the consumer's right to receive a listing of all disclosures of any PHI for the previous six years in which the information has been maintained. Tracking begins on the scheduled compliance date of April 14, 2003. Accounting is not required for disclosures made before that date.

The accounting for each disclosure must include: the date, name and address of the entity receiving the PHI; a brief description of what was disclosed; and a brief statement of the purpose of the disclosure. An accounting must be made within 60 days of the request for accounting. Consumers have the right to receive one free accounting per twelve-month period. For each additional accounting, a reasonable cost-based fee may be charged.

Consumers do not have the right to accounting for disclosures made:

- To health oversight or law enforcement agencies under special circumstances when such a disclosure might impede the agency's activities
- To persons involved in the consumer's care
- For national security and intelligence purposes
- To correctional institutions
- About their own access to their records or disclosures made pursuant to their authorization
- To HHS regarding compliance under the privacy rule
- To business associates
- To personal representatives (guardians)

RETALIATORY ACTION

A provider may not intimidate, threaten, coerce, discriminate or take other retaliatory action against a consumer for:

- Exercising a right or participating in any other allowable process under the privacy rule
- Filing an HHS compliance complaint
- Testifying, assisting or participating in a compliance review, proceeding or hearing
- Opposing any act or practice in which the consumer or their representative has a good-faith belief that the practice is unlawful and where the manner of opposition is reasonable and does not involve disclosure of PHI

WAIVER OF RIGHTS

Consumers cannot be required to waive their right to file an HHS compliance complaint as a condition of the provision of treatment.

BUSINESS ASSOCIATES

PHI may be disclosed to a business associate (a person or entity providing services on behalf of the covered entity). A business associate contract must clearly establish what is permitted and required regarding use and disclosure of records. Subcontractors must also agree to all of the contract's conditions and restrictions.

In effect, the provider needs to contractually obligate the business associate to follow all the HIPAA compliance requirements that the provider is required to follow.

If a provider knows that a business associate is breaching or violating an obligation under their contract, the provider has to take reasonable steps to cure the breach. If those steps are unsuccessful, the provider either must terminate the contract or, if that is not possible, report the problem to HHS.

MARKETING

Marketing is defined by the privacy rule to mean the making of a communication about a product or

service for the purpose of encouraging recipients to purchase or use that product or service. In general, authorization is required before a provider is able to use or disclose PHI for marketing purposes.

No authorization is required when using or disclosing PHI to make a marketing communication to an individual when the communication occurs in a face-to-face encounter with the individual.

FEDERAL SUBSTANCE ABUSE CONFIDENTIALITY REQUIREMENTS

The federal confidentiality of substance abuse patient records statute establishes confidentiality requirements for patient records that are maintained in connection with the performance of any federally assisted specialized alcohol or drug abuse program. According to an analysis conducted by HHS of the interaction of this law (and regulations) with HIPAA, in most cases a conflict will not exist and health care professionals covered by both will be able to comply with both sets of requirements.

POLICIES AND PROCEDURES

New policies and procedures must be implemented with respect to PHI to comply with the requirements of the privacy rule. These policies and procedures must be promptly changed, as necessary and appropriate, to comply with any changes in the law that might occur in the future.

ADMINISTRATIVE AND PHYSICAL SAFEGUARDS

Appropriate administrative, technical and physical safeguards must be in place to protect the privacy of PHI. Additional requirements will take effect 26 months after the HIPAA Security Regulations are published in final form.

TRAINING

All members of a workforce must be trained as necessary and appropriate to carry out their functions under the privacy rule. Training must be documented in accordance with the rule's documentation requirements.

SANCTIONS

HIPAA requires a provider have and apply appropriate disciplinary sanctions against employees who fail to comply with the privacy policies and procedures or requirements of the privacy rule. Sanctions must be documented in accordance with the privacy rules documentation requirement.

COMPLAINT PROCESS

A consumer complaint process regarding compliance with the privacy rule or policies and procedures related to the rule must be in place. This may be as simple as receiving complaints and keeping a file of such complaints.

DOCUMENTATION OF COMPLIANCE PROCEDURES

Policies and procedures must be maintained in either electronic or written form. Various types of HIPAA documentation must be retained for six years from the date of creation or the date when it was last in effect, whichever is later.

DUTY TO MITIGATE

A provider must mitigate to the extent practical any harmful effect that is known about regarding an employee(s), or business associates use or disclosure of PHI in violation of policies and procedures or the requirements of the privacy rule. For example, if the wrong patient records are inadvertently sent to an insurer for reimbursement, the provider might be required to request the records back and inform the patient about the error.