Continuing Education

They're Real and They're Here: The New Federally Regulated Privacy Rules under HIPAA

Marilyn Frank-Stromborg

The purpose of the HIPAA Privacy Rules was to create national standards to protect the privacy of personal health information. As of April 14, 2003, all covered health care entities must comply with the newly implemented national standards. The importance of staying updated with the law, while particularly important for the patient's privacy, is just as important for the nurse to avoid civil punitive damages and possible criminal charges.

The Health Insurance Portability and Accountability Act (1996) was part of a Congressional effort at health care reform. The "portability" part of the Act was designed to minimize barriers to health coverage for workers. The regulations to minimize barriers to health coverage included (a) limits on excluding coverage for pre-existing conditions, (b) special enrollment rights for those who lose other health coverage, and (c) elimination of medical underwriting in group health plans (Claire, 2002). Congress then added nondiscrimination regulations called Privacy Rules. The purpose of the HIPAA Privacy Rules was to create national standards to protect the privacy of personal health information.

The Final Version of HIPAA

Making the Privacy Rules a reality, the Department of Health and Human Services (DHHS) issued its final version of the Privacy Rules on August 14, 2002, under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. As of April 14, 2003, all covered health care entities must comply with the newly implemented national standards. However, compliance for smaller health care entities with annual receipts of $5 million or less is extended until April 14, 2004 (45 CFR §§ 164.534, 164.160.103, 2002). Preparation for compliance of the final version of the Privacy Rules can be extensive given its particularity. Further, the final version means that the government is serious about the newly promulgated rules. In fact, the government is so serious concerning compliance with the Privacy Rules that not only can an employer be penalized with punitive damages, but personal punitive damages can also be a consequence of noncompliance. Therefore, the importance of staying updated with the law, while particularly important for the patient's privacy, is just as important for the nurse to avoid civil punitive damages and possible criminal charges.

History of the Privacy Rules

While 85% of consumers believe privacy of medical information is "absolutely essential" (Maradiegue, 2002), it is estimated during a patient's typical hospital stay over 400 people are likely to see all or parts of the patient's medical record (Davis, 2001). Sensitive to the lack of patient privacy, Congress enacted HIPAA in 1996, but failed to pass legislation pertaining to medical privacy. HIPAA therefore required the DHHS to create and implement a national set of privacy rules, known as the Administrative Simplification Standards, to: (a) improve the efficiency and effectiveness of the health care system; (b) create national standards to protect patients' personal health information; and (c) provide patients increased access to their medical records (Helwig, 2002).

DHHS first issued the Privacy Rules in December 2000. Due to thousands of suggestions and comments, it subsequently made changes to address obstacles that would have had the effect of blocking patients' access to quality care. For example, the previous rules would have posed barriers to health care by requiring the sick patient to personally visit a pharmacy to sign paperwork before a pharmacist could review the patient's medical information to fill prescriptions (DHHS,

Marilyn Frank-Stromborg, EdD, JD, FAAN, *is a Distinguished Research Professor and Chair, School of Nursing, Northern Illinois University, DeKalb, IL.*

Note: *This article originally appeared in MEDSURG Nursing, 12(6), 380-385, 414 and is reprinted here with permission of the publisher.*

Note: *CE Objectives and Evaluation Form appear on page 21.*

2002). Under the final version of the Privacy Rules, HIPAA allows a pharmacist to use protected health information that is telephoned in by a patient's physician. Furthermore, the DHHS received over 11,000 public comments on the proposed modifications issued in March 2002. Incorporating the public concerns and suggestions, the DHHS adopted changes to form the final version of the Privacy Rule on August 14, 2002.

Who Must Comply with HIPAA's Privacy Rules?

The Privacy Rules encompass three types of covered entities: health care clearinghouses, certain heath care providers, and health plans. The DHHS has promulgated standards and charts to help determine exactly who is a covered entity.

Health care clearinghouse. An entity is a covered health care clearinghouse if the business or agency is either a private or public billing service, repricing company, community health management information system, or community health information system that receives, processes, or facilitates the processing of health information from nonstandard format or content into standard format and performs this function for another legal entity (45 CFR § 160.103, 2002).

Health care providers. A health care provider who transmits any health information in electronic form in connection with covered transaction must comply with the Privacy Rules. *Health care* means, but is not limited to, any 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. It also includes the sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription (45 CFR § 160.103, 2002). Simply stated, the definition of health care provider encompasses and subjects a vast majority of practitioners of the medical field to the Privacy Rules.

Private benefit plan. Determining whether a private benefit plan is a covered entity requires more analysis. The definitions of health plans include HMOs, as well as various types of benefit plans sponsored by employers, such as medical, dental, vision, and prescription drug. However, some long and short-term disability plans are not covered by the rules, such as workers' compensation benefits, life insurance plans, and sick pay programs even though all entail employee health information. Furthermore, a health plan that has fewer than 50 participants and is self-administered is not a covered health plan for the purposes of the Privacy Rules (Stanton, Scheidt, & Bassler, 2002). Essentially anyone who uses health care or health insurance will be affected by the Privacy Rules, including, but not limited to, doctors, hospitals, health service organizations, health insurers, and employers who provide health insurance.

What Is Protected Under the Privacy Rules?

The purpose of the Privacy Rules is to protect the privacy of an individual's information taken for medical and insurance purposes. Because the payment and medical history of an individual is at the core of a person's intimate and private affairs, it should not be surprising that the Privacy Rules apply to all health information in oral, written, or electronic form that can be identified to a specific individual. Any health information, including demographic information that relates to the past, present, or future physical or mental health or condition of an individual, and with respect to which there is a reasonable basis to believe the information can be used to identify the individual, is protected information (45 CFR § 160.103, 2002).

It is important to note that individually identifiable information is protected health information (PHI) under the Privacy Rules when it is either transmitted or maintained by electronic form. Electronic form includes transmissions over the Internet, Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or CD media (45 CFR § 160.103, 2002).

The Privacy Rules also cover electronic transactions. Covered transactions include requests to obtain payment and necessary accompanying information from a health care provider to a health plan for health care. Covered transactions also include any inquiry from a health care provider to a health plan, or from one health plan to another health plan, to obtain any of the following information about a benefit plan for an enrollee:

- Health care claims or equivalent encounter information.
- Health care payment and remittance advice.
- Coordination of benefits.
- Health care claim status.
- Enrollment and disenrollment in a health plan.
- Eligibility for a health plan.
- Health plan premium payments.
- Referral certification and authorization.
- First report of injury.
- Health claim attachments.
- Other transactions that the Secretary may prescribe by regulation (45 CFR § 160.103, 2002).

Privacy Rights Of the Individual

The Privacy Rules of HIPAA

allow the individual to regain control over individually identifiable health information. The individual is guaranteed right of access to inspect and obtain a copy of PHI within 30 days of a request. If the covered entity denies the request in whole or in part, it must provide the individual with a written denial specifying the reasons for the denial, which is appealable by the individual (45 CFR § 164.524, 2002).

In addition, the individual also has the right to amend his or her PHI, such as medical records. If the entity fails to amend as specified by the individual, the individual may appeal this decision as well (45 CFR § 164.526, 2002). The individual must first make his or her appeal through the covered entity's administrative procedures. Thereafter, the decisions may be appealable to the Secretary of the DHHS.

An individual also has the right to receive an accounting of disclosures of PHI made by a covered entity for the last 6 years prior to the date the accounting is requested. Although there are some exceptions, the individual's request for the accounting must be produced within 60 days of the request (45 CFR § 164.528, 2002).

Perhaps one of the most significant controls the individual has over his or her PHI is the ability to request restrictions on a covered entity's use and disclosure of PHI, even when the rules allow otherwise. While a covered entity is not required to agree to an individual's requested restriction, in the event the entity does agree to the restriction, the covered entity can only use or disclose the information for emergency treatment purposes. Furthermore, the restriction can only be terminated by the individual or the covered entity, but only after the individual is informed of the termination (45 CFR § 164.52, 2002).

Allowed Uses and Disclosures Of PHI by Covered Entities

Although the Privacy Rules were promulgated with the patient's privacy interests in mind, the rules also recognize that the covered entity must be given some flexibility to effectively perform its services. The Privacy Rules allow a covered entity to use or disclose PHI to the individual upon his or her request. The rules also allow the covered entity to use and disclose PHI for the covered entity's own "treatment," "payment," or "health care operations" for the individual. In other words, any procedure or scheduling that falls under the definitions of "treatment," "payment," or "health care operations" exempts a covered entity from first obtaining the patient's consent before using or disclosing the patient's PHI for treatment of the patient. For example, health care providers, such as a specialist or hospital, may set up appointments or schedule procedures such as surgeries by using the patient's PHI without his or her consent because appointments and scheduling fall under the "treatment," "payment," or "health care operations" exceptions.

In addition, the Privacy Rules also allow use and disclosure to another covered entity or a health care provider for "payment" activities and "health care operations" if that entity has had a previous relationship with the individual (45 CFR § 164.506, 2002). For example, health care providers can consult with other providers about a patient's condition without the patient's written consent, because consulting is within the HIPAA's Privacy Rule's definition of "treatment." Furthermore, the rules also allow disclosure in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person (45 CFR § 164.512, 2002).

Minimum Necessary Requirement of PHI

Although covered entities are allowed to use PHI without an individual's express consent for "treatment," "payment," and "health care operations," the Privacy Rules still impose restrictions. The rules provide that when a covered entity does use or disclose PHI or even requests PHI from another covered entity, it must still make reasonable efforts to limit PHI to the "minimum necessary" to accomplish the intended purpose of the use, disclosure, or request. However, the minimum necessary does not apply to the individual who requests his or her PHI, or to a health care provider for "treatment purposes" of the patient (45 CFR § 164.502, 2002). For example, a physician's office may still fax a patient's protected health information to another treating physician's office because this would fall under the "treatment" of a patient exemption. However, the covered entity must still have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. Therefore, the physician's office should first confirm that the fax number to be used is in fact correct. The fax machine should also be in a secure area to prohibit unauthorized access to faxed information.

In some circumstances the Privacy Rules may only allow an exhaustive list of what protected health information may be disclosed. For example, a covered entity may only disclose to law enforcement the following information for identifying a suspect: the name, address, date and place of birth, social security number, blood type, type of injury, date and time of treatment, date and time of death if applicable, and a description of distinguishing physical characteristics, such as hair color, eye, color, and gender (45 CFR § 164.502, 2002). All

other personally identifiable disclosures would be in violation of the Privacy Rules.

The Privacy Rules do allow a covered entity to de-identify information so that the information is no longer individually identifiable health information. Identifiers of individuals or of relatives, employers, or household members of the individual must all be removed, including but not limited to, name, address, zip code, city, birth date, admission date, discharge date, age, telephone number, fax number, electronic mail address, social security number, medical record numbers, vehicle identifiers, and pictures (45 CFR § 164.514, 2002). Once all individually identifiable information is removed, HIPAA Privacy Rules no longer apply to the remaining information. Thus, the information can be used for studies and research, and can even be electronically transmitted.

Employee Restrictions of PHI

One of the most significant protections HIPAA's Privacy Rules affords to the individual is the restriction of PHI to employees of a covered entity. Under the rules, a covered entity must have procedures in place to identify those persons or classes of persons in its workforce who need access to PHI to carry out their duties. Furthermore, the covered entity must make reasonable efforts to limit the access of such persons or classes of persons to only the categories to which access is needed and any conditions appropriate to such access. A covered entity must implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of disclosure for routine and reoccurring basis. For all other disclosures, a covered entity must develop specific criteria to limit the protected information, and review requests for disclosure on an individual basis in accordance with such criteria. Specifically, the rules forbid disclosing an entire record unless it is absolutely necessary to accomplish the purpose of the use, disclosure, or request (45 CFR § 164.514, 2002). If the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes, then the entire medical record may be used or disclosed. However, the Privacy Rules mandate that policies and procedures must be in place to specifically identify those persons or classes in the workplace that would be allowed access to an entire medical file.

Not only must a covered entity develop and implement standards to ensure only necessary amounts of PHI are disclosed to employees, but a covered entity must also provide training to each member of the covered entity's workforce by no later than the compliance date of either April 2003 or April 2004. A covered entity also must provide a process for individuals to make complaints concerning the entity's policy and procedures as it pertains to its employees' access to PHI. Furthermore, the Privacy Rules mandate that covered entities must have and apply sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity (45 CFR § 164.530, 2002). See Table 1 (pp. 384-385) for common HIPAA questions and answers related to specific clinical situations and necessary responses.

Authorizations Required

The Privacy Rules mandate authorizations for some uses and disclosures. For example, a covered entity must obtain a written and signed authorization from the individual for use or disclosure of psychotherapy notes. There are some exceptions to this rule, however. The originator of the psychotherapy notes may use its psychotherapy notes for treatment. A covered entity may also use or disclose its notes for its own training programs, and a covered entity may use or disclose its psychotherapy notes to defend itself in a legal action brought by the individual. An authorization is also required for any use or disclosure of PHI for marketing, with some minor exceptions (45 CFR § 164.508, 2002).

Beyond the requirement that the authorization must be in plain language, the Privacy Rules specify a detailed list of required statements that must be implemented in the authorization for it to be valid. Required elements of the authorization include: (a) a description of the information to be used or disclosed, (b) the name or class of persons who are authorized to make the requested use or disclosure, (c) the name or class of persons for whom the covered entity may make the requested use or disclosure, (d) a description of each purpose of the use of disclosure requested, (e) an expiration date that relates to the individual or the purpose of the use or disclosure, (f) statement that the authorization is revocable, and (g) signature of the individual (45 CFR § 164.508(c), 2002).

Notice Required To Individuals

The Privacy Rules are quite clear that the covered entity must give written notice to the individual of the allowed uses and disclosures of PHI, as well as the individual's rights as discussed previously, and the covered entity's legal duties. This notice must be written in plain language and the covered entity must retain copies of all issued privacy notices to prove compliance. In addition, the Privacy Rules incorporate a detailed list of specific requirements that must be included in the notice, including

Table 1.
Common HIPAA Questions and Answers

Faxing
Q. I am a public health nurse and we frequently have to fax questions to the private physicians taking care of our patients. What can be done?
A. Faxing health-related questions to private physicians is allowable under the Privacy Rules if it is for treatment of the patient. Treatment is defined as the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to a patient, or the referral of a patient for health care from one health care provider to another. However, the nurse should first confirm that the fax number is correct and make sure the fax is in a secured location to prevent unauthorized access.
Q. I work in a nursing home, and we have to fax patient records to doctors' offices all the time or have them fax orders to us. What are the limitations on this practice?
A. This is considered treatment and use and disclosure by fax is allowable, but proper administrative, technical, and physical safeguards must be provided to protect the individual's privacy.
Q. Can I fax information to pharmacies/MD offices from our hospital or physician offices such as patient lab values, and notes from other health care providers such as physical therapy, or consultants called into the case?
A. As long as the disclosures are being made for treatment purposes for the patient, the necessary disclosures are allowed to be faxed to other treating entities, including pharmacies. The Privacy Rules permit a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rules, such as treatment of the patient. However, the minimum necessary rule is always in play. The minimum necessary rule is based on the practice that protected health care information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.
Q. We work in the doctor's office and are always asked to fax information to the local hospital or other physician offices. What can we fax without worry?
A. As long as the requested information is for "treatment," "payment," or "heath care operations" of the patient, the requested information should be appropriate to fax. However, the minimum necessary rule is always in play. It is also necessary to ensure the appropriate administrative, technical, and physical safeguards.
Person-to-Person Conversations
Q. Will you get in trouble talking about cases in general over lunch?
A. Generally the answer is no, as long as specific names or specific identifying information could not be overheard by those who are not supposed to be privy to such information. Reasonable precautions must always be taken to minimize the chance of incidental disclosures to others who may be nearby, such as lowered voices or talking apart from others when sharing protected health information.
Q. If family members want information on a patient, will this law prevent our talking to them? Will we have to get special permission to talk to family members about the health of their loved one? Will this end the practice of family members telling us that they don't want their mom or dad to have the news about their diagnosis?
A. The Privacy Rules permit health care providers to communicate with family members, but to a limited degree. While the Privacy Rules permit covered entities to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present, the covered entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed. Health care providers are allowed to communicate with patients at their homes by either leaving messages on an answering machine or with a person at the patient's home. However, to reasonably safeguard the individual's privacy, providers should take care to limit the amount of information disclosed on the machine or with a person. For example, the representative of a covered entity might want to consider leaving only its name and number and other information necessary to confirm and appointment, or ask the individual to call back.

Table 1. (continued)
Common HIPAA Questions and Answers

Phone Conversations
Q. Will nursing staff still be able to call in prescriptions into the pharmacy and talk about specific patients on the phone?
A. Yes. In these circumstances, however, reasonable precautions would include using lowered voices and talking apart from others when sharing protected health information. Nurses should use phones that are not in an open area where bystanders and/or other patients could hear an individual's protected health care information when being phoned into the pharmacy.
Q. Do the rules change anything about nurses phoning patients about their lab values or scans? Talking to family members about this and leaving messages?
A. Yes and no. Nurses are still permitted to phone patients to give results. However, talking to family members is different. Remember that not all family members share their health information with one another. Assuming this could get you in trouble. The rules allow limited disclosure. A covered entity may disclose to a family member, other relative, or any other person *identified* by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's care. If the individual is not present or the opportunity to agree or object to the use of disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether disclosure is in the best interests of the individual, and if so disclose only the protected health information that is directly relevant to the person's involvement. Therefore, if there is no expressed consent, it is better to err on the side of caution and wait to talk to the patient himself if feasible.
E-mails
Q. Can we e-mail specific information about patients such as names and lab values between providers? What about leaving voice mail or patient information?
A. E-mails and voice mails can technically still be disclosed between treating providers; however, stricter safeguards should be enforced. In the event protected health care information of a patient is received by a wrong recipient through e-mail, the sending provider will be in violation and possible civil and criminal penalties could follow. Voice mails are most likely more secure than some email accounts, but the provider must always make sure the recipient is the intended recipient to avoid violations.
Receiving and Providing Patient Information
Q. How do we handle situations where the patient is not present in the health care facility to give permission but we need the information from another health care institution the next day or in a couple of days?
A. Under the old version of the Privacy Rules, this would have been a big problem. However, the final version of the rules allows use and disclosure of a patient's medical information for treatment purposes. Therefore, physical presence and consent by the patient is not necessary for one provider to receive a patient's medical information from another provider for treatment purposes. As always, the minimum necessary standard is in play as well as safeguards against the information going into the wrong hands.
Benefits of HIPAA
Q. What do you see as the real downside and the upside of HIPAA? Isn't it really going to mean more work for health care professionals?
A. As with any new rule or regulation, the learning process will take time and patience from both the covered entities subject to the rule as well as the individuals. However, once the system is in full swing, there should be many benefits to safeguard a person's most intimate information: 1. It gives patients more *control* over their health information. 2. It sets *boundaries* on the use and release of health records. 3. It establishes appropriate *safeguards* that health care providers and others must achieve to protect the privacy of heath information. 4. It holds violators *accountable*, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.

Note: The above questions and answers were taken from U.S. Department of Health and Human Services, Office for Civil Rights-HIPAA. *Medical privacy-national standards to protect the privacy of personal health information.* Retrieved December 6, 2002, from http://www.hhs.gov/ocr/hipaa/privacy.html

a description of the types of uses and disclosures allowed to be made with and without the individual's written authorization, and the effective date of the notice. In addition, the individual must be informed that he or she may complain to the covered entity and to the Secretary of the DHHS if the individual believes privacy rights have been violated (45 CFR § 164.520, 2002). However, the individual must file a complaint within 180 days of when he or she knew or should have known that privacy rights were violated.

The notices were to have been sent to all current patients and individuals by April 14, 2003, for most covered entities. As previously stated, small health care entities with $5 million or less in annual receipts have until April 14, 2004, to comply with the Privacy Rules. Thereafter, privacy notices are due no later than the date of the first service delivery for new patients and individuals (45 CFR § 164.520, 2002).

HIPAA Enforcement

A covered entity's failure to comply with the rules, intentionally or even unintentionally, could have ramifications of civil and even criminal penalties. Congress has prescribed civil penalties of $100 per noncompliance occurrence, up to $25,000 per calendar year. Congress has also granted the DHHS the power to alert the Justice Department for criminal prosecution that could result in criminal penalties up to $50,000, and/or up to 1 year in jail. A criminal violation can include wrongful disclosure of individually identifiable health information. In the event such wrongful disclosure is made under false pretenses, criminal penalties of imprisonment up to 5 years and fines up to $100,000 could result. Finally, criminal penalties of up to $250,000 and up to 10 years in prison can result for obtaining or disclosing private health information with the intent to sell for personal gain, commercial advantage, or malicious harm (42 USC §§ 1320d-5, 1320d-6, 2002).

Conclusion

While most, if not all, health care professionals will likely be affected by HIPAA's Privacy Rules, they should remember that the purpose is to uphold and protect the right to privacy afforded by the First Amendment of the Constitution. Although the Privacy Rules will undoubtedly restrict a covered entity's uses and disclosures of PHI, limitations are all in the name of protecting privacy of individuals. After all, 85% of consumers feel privacy of medical information is absolutely essential. HIPPA's Privacy Rules is the tool to ensure those privacies.

References

Claire, P.F. (2002). *The HIPAA privacy rules: What every employer needs to know.* Retrieved May 20, 2003, from http//www.willinghamcote.com/articles/pfc-hipaaprivacyrules.htm

Code of Federal Regulations. (2002). 45 CFR Parts 160 and 164. *Standards for privacy of individually identifiable health information.* Retrieved December 6, 2002, from http://www.hhs.gov/ocr/hipaa/privacy.html

Davis, K.B. (2001). Privacy rights in personal information: HIPAA and the privacy gap between fundamental privacy rights and medical information *John Marshall Journal of Computer and Information Law, 19,* 535.

Helwig, A. (2002, May). HIPAA primer: What you need to know now? *Mdnetguide.* Retrieved August 22, 2003, from http://www.mdnetguide.com

Maradiegue, A. (2002). The Health Insurance Portability and Accountability Act and adolescents. *Pediatric Nursing, 28*(4), 417-420.

Stanton, T.J., Scheidt, K.S., & Bassler, S.A. (2002). *What every employer needs to know about the HIPAA privacy rules.* Retrieved May 19, 2003, from http://www.gcd.com

U.S. Department of Health & Human Services. (2002). *HHS Issues first major protections for patient privacy: Consumer gain new controls over records beginning April 2003.* Retrieved May 19, 2003, from www.hhs.gov/news/press/2002pres/ 20020809a.htm