HIPAA Privacy Rule: The Debate Continues

KARRIE B HOVIS, DIANNA M VEILLON

ABBREVIATIONS: DHHS = Department of Health and Human Services; HIPAA = Health Insurance Portability and Accountability Act; LIS = laboratory information system; PHI = protected health information; POL = physician office laboratory.

INDEX TERMS: HIPAA.

Clin Lab Sci 2003;16(2):85

Karrie B Hovis CLS(NCA), *is an Instructor,* ***Dianna M Veillon MD*** *is an Associate Professor, Louisiana State University Health Sciences Center, Shreveport LA.*

Address for correspondence: *Karrie B Hovis CLS(NCA), Louisiana State University Health Sciences Center, 1107 Mountainbrook Dr, Shreveport LA 71118. (318) 675-6807, (318) 675-6937 (fax). Khovis@lsuhsc.edu*

The Fourth Amendment of the United States Constitution guarantees that "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated." In other words, the Fourth Amendment guarantees the privacy of Americans. Yet, many Americans feel that this freedom has been violated when discussing the privacy of their medical information. They are concerned that the privacy of their medical information is not protected. In January 1999, a national survey conducted by the California HealthCare Foundation found that one in five Americans feel that their health information is being disclosed inappropriately. Without this trust, patients are compromising their own healthcare either by providing inaccurate information to their physician, changing physicians, or avoiding care altogether.[1] With the rising concern about patient privacy, the United States federal government realized that something needed to be done.

The peer-reviewed Clinical Practice section seeks to publish case studies, reports, and articles that are immediately useful, of practical nature, or demonstrate improvement in the quality of laboratory care. Direct all inquiries to Bernadette Rodak MS CLS(NCA), CLS Clinical Practice Editor, Clinical Laboratory Science Program, Indiana University, Fesler 409, 1120 South Avenue, Indianapolis, IN 46202-5113. brodak@iupui.edu

On August 21, 1996, the Health Insurance Portability and Accountability Act (HIPAA) was enacted. Although this legislation was well intended, its supporters failed to recognize several potential problems. One of the biggest shortfalls was the fact that patient health information may be exposed without patient consent. Even though all states had laws in effect to cover this deficit, the laws varied from state to state. The Department of Health and Human Services (DHHS) has subsequently issued another law entitled the HIPAA Privacy Rule. This law is expected to prevent exposure of a patient's confidential medical information. New questions have arisen. Should the HIPAA Privacy Rule override current state legislation? Has the federal government overstepped its boundaries this time?

When HIPAA was first enacted, its primary purpose was to ensure that all workers who lost or changed jobs were able to maintain health insurance. The law, however, included significant changes concerning fraud and abuse in healthcare and encouraged the establishment of medical savings accounts. HIPAA also attempted to simplify the administration of health insurance by encouraging electronic transmission of certain transactions.[2] By allowing these electronic transactions to occur, the government was expected to save $29.9 billion over ten years.[3] In all the calculations of potential savings, however, the cost of regulation was not included. By allowing electronic transactions to occur, the federal government introduced another problem: patient privacy. With concerns of patients' protected health information (PHI) being exposed, the government had to issue another set of regulations to cover this deficiency. This set of regulations is included under the HIPAA Privacy Rule.

Several groups are affected by the implementation of the HIPAA Privacy Rule. Any organization that transmits patient health information electronically is considered a covered entity under the HIPAA Privacy Rule. These organizations include health plans, healthcare clearinghouses, and healthcare providers. Most group health plans, health insurance carriers, health maintenance organizations (HMOs), and federal health programs are included. Therefore, if you are a recipient of Medicare benefits, the Privacy Rule will protect your PHI.[4]

Clearinghouses are organizations that are considered the 'middle man' of insurance claims. They are responsible for translating data received from the payee to the payor. In other words, an insurance claim that is received electronically from a hospital undergoes data translation before the final bill is sent to the patient. The healthcare clearinghouse is responsible for the interpretation and the billing process. Controversially, some clearinghouses are selling their gathered information to the private sector. For example, pharmaceutical companies frequently purchase information from these clearinghouses for research purposes and market analysis.[4]

Healthcare providers include physician offices, pharmacies, and hospitals. A healthcare provider is defined as "a provider of healthcare, medical, or health services as defined in the Act (HIPAA), or any other person or organization that furnishes, bills for, or is paid for healthcare services or supplies in the normal course of business".[4]

According to the Privacy Rule, a covered entity must make "all reasonable effort" not to disclose patient information that will not be used for the intended purpose. This requirement is referred to as the "minimum necessary" rule. Under this rule, a covered entity must be careful about which patient information is made known, but this has the potential to jeopardize patient care.[5] Although a trustworthy physician/patient relationship is essential, limiting the use of information while trying to provide adequate services can potentially present a problem.

If a covered entity must disclose patient information to an outside source who is a business associate, a confidentiality contract must be reached beforehand. Not only does this create more paperwork, but also the covered entity is held liable for breach of patient information if the contract is not upheld. Although the covered entity need not actively monitor the outside source, they must ensure that all business associates adhere to the original contract. It is the responsibility of the covered entity to adopt written privacy procedures to address this issue and to investigate credible evidence of contract violation.[3]

The HIPAA Privacy Rule also introduced the term "privacy officer". Each covered entity must appoint someone to fulfill this position. The purpose of this individual is to ensure that the entity's privacy procedures are followed.[3] In many cases, this responsibility will be delegated to an individual who already has several compliance duties. On October 22 2001, two congressmen, Representatives John Peterson (R-PA) and John Murtha (D-PA), urged Congress to work with the DHHS to reduce the burden that HIPAA is placing on the healthcare community. They wanted "to see that the final (HIPAA privacy) regulations do not get in the way of the heroic work that hospitals do every day."[6]

One advantage to the HIPAA Privacy Rule is that individuals will be able to inspect, copy, and request changes to their medical records. Many state privacy laws currently address this issue as well. Under the HIPAA regulations, the covered entity will be allowed to charge a fee to offset copying expenses. This could create a hardship for the poor.[5]

Another problem with individuals inspecting their medical records is the refusal of the covered entities to make any changes to the records. Covered entities will need to devise guidelines for changing or refusing to change medical records. For example, a patient might request a change in the date of a service if the service predated his/her insurance coverage.[4] Although the covered entity is correct in refusing the change, this could precipitate a conflict.

Where does the clinical laboratory fit into the picture of patient privacy? We are professionals who provide a service for the patient, and we bill for that service. Therefore, this classifies the laboratory as a healthcare provider. However, there are two types of healthcare providers: direct and indirect. For the most part, clinical laboratories are going to be considered indirect healthcare providers. Most clinical laboratories, such as hospital laboratories and reference laboratories, have an indirect relationship with the patient.[7] As laboratorians, we interact with the physician, not the patient. The Privacy Rule does not require clinical laboratories to provide patient access to laboratory results since the Clinical Laboratory Improvements Amendments of 1988 (CLIA '88) prohibits this service. Patients can only inspect and copy their laboratory results through the healthcare provider. The only exception to this rule is if state law permits patients to gain access to laboratory results. If the state law defines an "authorized person" to include the patient, then the patient can gain access of their laboratory results through the laboratory personnel.[8]

POLs are in a direct relationship with the healthcare provider. Due to their location, these laboratory personnel offer their services directly to the patient. Therefore, it is imperative that these facilities have policies and procedures in place to address the concern of patient privacy.

As for research laboratories, the privacy regulations still apply but have different applications. For instance, some laboratory results can be released directly to the patient in a research setting. If the laboratory result will not be used for purposes of diagnosis or treatment, then the patient can receive the laboratory result without having to go through the ordering individual.[8]

Should the laboratory offer a separate consent form? According to the HIPAA Privacy Rule, a separate consent form is not needed. We perform a service for the patient, but the doctor requests the service. The argument has been made that in states where the state law permits the patient to gain access directly to the laboratory results then a consent form (or some other legal document) should be necessary.[9] Numerous instances have been reported in which laboratory professionals released results directly to the patient. In some cases, a consent form was signed, but in most, there was no documentation made. Before any results are released directly to the patient, laboratory professionals should have knowledge about what their state law allows.

Other practices, such as the reporting of communicable diseases to public health authorities, are excluded from the Privacy Rule.[8] It is the responsibility of clinical laboratory personnel to report such findings as methicillin-resistant *Staphylococcus aureus* to the public health officials. Such findings are required by law for the purposes of public health and will continue to be reported without a confidentiality contract.

As for significant changes that will directly affect all laboratory personnel, there will be few. The HIPAA Privacy Rule will now regulate all current and historical data stored in an institution's laboratory information system (LIS). Changes in transaction codes that will be implemented by the LIS vendor may require some computer downtime.

Some LIS vendors require facilities to release protected health information in order to troubleshoot problems. This practice will become more limited with the new privacy regulations. Also, more stringent rules will be put in place for employees to gain access to facility-wide systems. This access will be granted on a 'need to know' basis. All healthcare professionals will be required to undergo some form of privacy training at their facility as part of compliance. Some facilities may require employees to document and keep copies of all facsimile transmission reports. This is to ensure that the right person received the report. Fax numbers may also have to be verified before transmission.[10]

Currently, there is a meshwork of state laws that address this issue. While several states have laws that enforce very strict confidentiality regulations, some states have laws that are more lenient. Thus, there is no uniformity involving the protection of a patient's PHI. The HIPAA Privacy Rule is the federal government's first attempt to govern the privacy of PHI. According to the DHHS, this rule will provide the groundwork for regulation of a patient's health information.[5]

Some state laws conflict with the Privacy Rule and also with each other. The Privacy Rule will supersede any state laws that are not sufficiently strict. A major concern is that certain areas of the country have situations that are not conducive to the federal law. Federal legislation does not address a population's specific needs. On the other hand, insurance companies, who frequently operate across state lines, are very much in favor of federal regulations. They claim that allowing federal regulations to override state laws will result in decreased costs to the consumer.[5]

Most Americans agree that we are in desperate need of more strict confidentiality regulations. Before the Privacy Rule was issued, our employers could gain access to our health records. A patient's entire medical record could be released to an employer even if only a portion of the information was requested.[5] In the past, this practice has affected hiring and promotion. However, with the new privacy law in place, people are now scared that the government will have more access to their health records.[11] The Office for Civil Rights (OCR) can access an individual's PHI without his/her consent if there is reason to suspect that the Privacy Rule has been violated.[12] The Food and Drug Administration (FDA) can also access patient information in effort to regulate "the quality, safety, or effectiveness of FDA-regulated products or activities".[13]

On April 14, 2003, the nation's healthcare system will have to be in compliance with the HIPAA Privacy Rule. Many organizations will have difficulty meeting this deadline. For some, the problem will be lack of preparation.[11] For other organizations, the problem may be a more personal decision to prevent more governmental control over our nation's healthcare system. The Privacy Rule is a popular item of debate, and both sides of the debate are condemnatory of the rules.[5] Whatever the outcome, the delivery of healthcare will be different, and the change will be felt by many.

REFERENCES

1. U.S. Department of Health and Human Services. Final Privacy Rule Preamble. http://aspe.hhs.gov/admnsimp/final/PvcPre02.htm. Accessed May 12, 2002.
2. Countryman C, Jahnke HC, Mohre EH, and others. Privacy Officers Association, and American Health Information Management Association. HIPAA compliance handbook-electronic transactions and privacy standards. Gaithersburg, Maryland: Aspen Publishers; 2001:1-2.
3. U.S. Department of Health and Human Services. HHS fact sheet-protecting the privacy of patients' health information. http://aspe.hhs.gov/admnsimp/final/pvcfact2.htm. Accessed February 10, 2002.
4. Roach MC. HIPAA privacy: individual rights and the minimum necessary requirements. J Health Law 2000;33:551-74.
5. Hussong SJ. Medical records and your privacy: developing federal legislation to protect patient privacy rights. Am J Law Med. 2000;26:455-74.
6. American Hospital Association. HIPAA standards-advocacy materials. http://www.aha.org/hipaa/advocacy.asp. Accessed February 3, 2002.
7. Boothe J. HIPAA privacy rule issued: the clock is ticking, Part One. Vantage Point 2001;5:1-9.
8. Office for Civil Rights. Section by section of rule provisions. http://www.hhs.gov/ocr/part2.html. Accessed October 24, 2002.
9. Boothe J. HIPAA privacy rule issued: the clock is ticking, Part Two. Vantage Point 2001;5:1-6.
10. McMahan J. HIPAA, Your LIS, and you. Adv Med Lab Professionals. 2002;14(7):8.
11. Rosati K. The HIPAA privacy guidance: preview of a "reasonable" enforcement posture. Health Law Dig 2001;29:3-11.
12. Office for Civil Rights. Standards for privacy of individually identifiable health information [45 CFR Parts 160 and 164]. OCR Rights. Fact Sheet: modifications to the standards for privacy of individually identifiable health information — final HIPAA Privacy TA 164.000.001. July 6, 2001.
13. Office for Civil rule. http://www.hhs.gov/news/press/2002pres/20020809.html. Accessed October 24, 2002.