Seymour Katz, M.D., Series Editor

HIPAA and the Privacy Rule: What Clinical Investigators Need to Know

by Marilyn R. Carlson

Editor's Note: The burst of new and novel therapies in inflammatory bowel disease have been critically dependent on clinical trials. Although the emphasis on safety and efficacy of such trials is clearly articulated, the components of patient protection (i.e., privacy of confidential data and a truly informed consent) are not often well delineated.

Dr. Carlson highlights the features of both the legal and ethical constraints necessary for the conduct of clinical trials in a clearly practical manner. Her remarks represent a welcomed addition of confidentiality requirements to the safety and efficacy concerns of research involving patient participation.

Seymour Katz, M.D., Series Editor

In addition to obtaining Informed Consent prior to enrolling subjects in clinical trials, Investigators are now required to obtain written permission from these individuals to use and/or disclose their protected health information for research purposes. This relatively new requirement is a provision of HIPAA entitled Standards for Privacy of Individually Identifiable Health Information or, as it is more commonly known, the Privacy Rule. Physicians involved in clinical research need to be aware of the Privacy Rule, what it intends to accomplish, who is required to comply, exceptions to the Rule, enforcement and penalties for non-compliance. This article summarizes key features and provides practical suggestion for incorporating these requirements into the conduct of studies that are planned, on-going or completed.

BACKGROUND AND INTENT

Standards for Privacy of Individually Identifiable Health Information or the Privacy Rule is a federal law that implements the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA guaranteed insured individuals that their health insurance coverage would be portable when they changed employers or health plans. The stated goal of the Privacy Rule is to assure protection of the privacy of an individual's health information while permitting the flow of information needed to provide quality health care and to protect the public health and well-being (1).

The Privacy Rule, referred to as simply as "the Rule," became effective in April of 2003 and set the minimum privacy standards at the federal level. In states

(continued on page 68)

Marilyn R. Carlson, D.M.D., M.D., RAC, President, entreMeDica, Inc., Encinitas, CA.

(continued from page 66)

where privacy laws are more stringent, those laws govern (2). Compliance with the Rule requires that an investigator obtain written authorization from individuals before using or disclosing their protected health information (PHI) for research purposes. In order for the written authorization to be considered valid, the Rule also specifies the information that must be included. These are referred to as the "core" elements of the authorization.

According to the Rule, a valid authorization describes **what** information will be disclosed, it describes **how** the information will be used or disclosed, **by whom** and **to whom** the information will be disclosed, until **when** (the expiration date), who authorizes disclosure and use (the individual's signature and date the document was signed). Three additional required statements include; the right to revoke authorization in writing, consequences of not giving authorization (i.e., whether research-related treatment requires authorization), and the potential the recipient may not be covered by the Privacy Rule and may re-disclose protected health information. The authorization must be in plain language and a copy must be provided to the individual giving authorization.

Since the authorization focuses on privacy risks, it differs from the Informed Consent. The Informed Consent describes the study, the anticipated risks and/or benefits associated with participation in the study, and how the confidentiality of the records will be maintained. The Rule allows the two documents to be combined into a single document as long as the required core elements and statements are included, however, not all states permit the two documents to be combined.

The Privacy Rule does not require the institutional review board (IRB) to review the authorization document. However, if the authorization is combined with the Informed Consent in one document requiring one signature, the IRB will review the document in its entirety.

The Rule also gives individuals the right to access their PHI, including information created or obtained in the conduct of a clinical trial. The individual's access to PHI may be temporarily suspended when the research is in progress provided; 1) the individual has agreed to a denial of access when consenting to participating in the research and, 2) the covered health care provider has informed the individual that the right of access will be re-instated upon completion of the research (3).

WHO IS REQUIRED TO COMPLY

The Rule applies to "covered entities" defined as health plans, health care clearinghouses and health care providers who transmit health information in electronic form in connection with a transaction for which the Department of Health and Human Services (HHS) has adopted a standard. This includes health care providers who furnish, bill or are paid for health care in the normal course of business. Therefore, the majority of physicians in clinical practice will be required to comply with the Rule if they also conduct studies or administer experimental therapies to participants during the course of a study (2).

EXCEPTIONS

Although the Privacy Rule prohibits use and disclosure of PHI for research purposes without written authorization, there are a limited number of exceptions (4). A summary of these exceptions is provided.

Not a Covered Entity

If a researcher is not considered a covered entity, the Privacy Rule does not apply.

Preparation for Research

The purpose of PHI use or disclosure is to prepare for performing the actual research and PHI will not be removed from the site. This is classified as a review preparatory to research and written authorization is not required.

PHI Collected Before the Privacy Rule

PHI collected under Informed Consent prior to April 14, 2003, can be used and disclosed for research purposes without an authorization.

This does not change the Rule for retrospective studies. Researchers conducting retrospective studies—even those that only involve data re-analysis—are required to obtain either written authorization or a waiver from an IRB/Privacy Board.

Research Using a Decedent's Information

The Rule allows covered entities to disclose the PHI of deceased individuals to researchers for research purposes. Prior to doing so the covered entity must obtain

(continued on page 70)

(continued from page 68)

assurance that the disclosure is necessary, that the research is on the deceased individual's PHI, and, if requested, documentation of the death of the individual.

In this situation state laws may be more stringent than the Privacy Rule. If so, state law governs.

IRB/Privacy Board Waivers

An IRB or a Privacy Board *may* waive the requirement for a signed authorization by a study participant if the following apply:

- use or disclosure of the PHI involves no more than minimal risk that the individual could be identified,
- research could not be practicably carried out without the waiver,
- research could not be conducted without access to the PHI,
- the research data has been de-identified.

DE-IDENTIFYING PHI

Under the Privacy Rule, PHI may be de-identified in several ways.

The Rule allows a covered entity to de-identify data by removing all 18 elements that could be used to identify the individual, their relatives, employers or household members.

See Table 1 for a list of the 18 individual identifying elements.

Or, rather than remove all 18 individual identifiers, statistical methods may be used to de-identify the PHI. The person certifying statistical de-identification must document the methods used as well as the results of the analysis in written or electronic format. The covered entity is required to keep such certification for at least 6 years from the date of its creation or the date when it was last used whichever is later.

The information is a "limited data set" in which certain participant identifiers have been removed and there is a data use agreement between the researcher and the IRB.

ENFORCEMENT AND PENALTIES

HIPAA includes penalties for covered entities that misuse PHI. Within the U.S. Department of Health and Human Services, the Office for Civil Rights (OCR) is responsible for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

A covered entity that violates the standards set forth in the Rule is liable per incident up to $25,000 per person, per year, per standard. For covered entities that knowingly and improperly disclose information or obtain information under false pretenses for monetary gain or malicious harm, federal criminal penalties range from $50,000 and one-year in prison to $250,000 and 10 years in prison.

PRACTICAL TIPS FOR COMPLYING WITH THE PRIVACY RULE

Step One—Determine if the Privacy Rule Applies

The first step is to determine if you are considered a covered entity. To determine your covered entity status, a set of tools is available from HHS (5). Most practicing physicians who also participate in research involving humans will be required to comply with the Privacy Rule.

Step Two—Clarify Requirements for Compliance

Since the Privacy Rule sets the minimum federal standards for the protection of privacy, state and local laws may still apply. Depending on your clinical research setting and/or the funding for your study, there are resources available to identify what is needed to be in compliance.

Local resources include:

- The office of research within your university, hospital or health maintenance organization
- The Institutional Review Board (IRB) located within the organization
- Free-standing or independent IRBs that operate for profit and support clinical research sites not affiliated with institutional IRBs

Depending on the funding for your research, there are other resources that may be available. These include:

- National Institutes of Health (NIH)
- Non-government research sponsors including pharmaceutical companies and special interest groups

There are also numerous government publications on HIPAA, the Privacy Rule and implications for clinical research (2–4,6).

(continued on page 73)

(continued from page 70)

Table 1
Elements of Identifiable Health Information*

Identifiers of the Individual or of Relatives, Employers or Household Members

1. Names
2. Addresses including smaller geographic subdivisions than a state, more than first 3 digits of zip code
3. All elements of dates (except year) for dates directly relating to an individual; birth date, admission date, discharge date, date of death, all ages over 89
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers, serial numbers, license plate numbers
13. Device identifiers/serial numbers
14. Web universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers/finger prints/voice prints
17. Full face photographic images and comparable images
18. Any other unique identifying number, characteristic, or code, except as permitted by #3 above

*Source: U.S. Code of Federal Regulations [45CFR§164.514(a)]

Step Three—Designing the Authorization Document

The elements of the valid authorization lend themselves to a template that can be customized for your study. Templates may be available from an IRB.

Consider whether it is advisable, and permissible in your institution, to combine the authorization and the Informed Consent into one document.

Step Four—Obtaining Authorization and Informed Consent

Recent experience has shown individuals considering study participation may be very concerned about the privacy of their health information. If, after reviewing the authorization document, they have questions, it is important that knowledgeable staff is available to respond to these questions.

Privacy concerns have been known to shift the focus away from important safety information described in the Informed Consent. It is the investigator's responsibility to insure the potential study subject is encouraged to pay adequate attention to the study design, as well as the potential benefits and risks associated with study participation.

Some sites have found it helpful to prepare a script as well as answers to frequently asked questions for the study staff to use when obtaining authorization and informed consent. It is important to include adequate time for this process in the study budget.

SUMMARY POINTS

- The Privacy Rule supplements, but does not replace, regulations governing clinical research or local laws governing privacy.
- Effective April 2003, a covered entity can only use or disclose an individual's protected health information for treatment, for payment and for health care operations purposes.
- For all other purposes, including research, the covered entity must obtain written authorization from the individual prior to using or disclosing PHI, unless an exception applies.
- Although the Rule was not intended to regulate research, it does create additional responsibilities for the investigator and the study staff. ■

References

1. Full text of the *Privacy Rule.* HIPAA Privacy Web site of the Office for Civil Rights; http://www.hhs.gov/ocr/hipaa
2. *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule.* NIH Publication No. 03-5388, April 2003; http://privacyruleandresearch.nih.gov/pr_02.asp
3. *Clinical Research and the HIPAA Privacy Rule.* NIH Publication No. 04-5495, posted February 2004, last edited June 2004; http://privacyruleandresearch.nih.gov/pdf/clin_research.pdf
4. *Impact of the HIPAA Privacy Rule on Academic Research.* American Council on Education, November 2002; http://www.acenet.edu/washington/legalupdate/2002/hipaa
5. Centers for Medicare and Medicaid. Covered Entity Decision Tools. http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp
6. *Myths and Facts About the HIPAA Privacy Rule.* Health Privacy Project; Telephone: 202-721-5632; info@healthprivacy.org