Research and the HIPAA Security Rule

Prepared for the Association of American Medical Colleges

by

Daniel Masys, M.D.
Professor and Chairman, Department of Biomedical Informatics
Vanderbilt University School of Medicine

March 8, 2005

Research and the HIPAA Security Rule

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] contains provisions that have important implications for biomedical researchers and academic health centers. The HIPAA Privacy Rule, for which compliance was mandatory effective April of 2003, defined the types of organizations (called Covered Entities) that are subject to HIPAA and the concept of Protected Health Information, which is person-identifiable health data arising out of health care operations within Covered Entities. The Privacy Rule specified that PHI could be used, created or disclosed for research purposes only if authorized by a signed authorization, or waiver of that authorization by an Institutional Review Board or Privacy Board. The HIPAA Security Rule, for which compliance the compliance date is April 20, 2005 may potentially have much more significant impacts on the cost and ability of academic health centers to conduct research using person-identifiable data elements.

Security Rule: Basic Concepts

Like the Privacy Rule, the Security Rule affects Covered Entities (CEs) that create, store, use or disclose Protected Health Information (PHI). Unlike the Privacy Rule, the Security Rule affects only PHI in electronic format (ePHI), not oral or paper-based PHI. The Security Rule applies security principles well established in other industries, and the level of effort to implement security will depend on the size and complexity of the organization. Rather than dictate specifics of technology implementation, the Security Rule emphasizes security management principles and broad management controls as the primary vehicles for protecting ePHI. The Rule specifies required and "addressable" standards. There are 17 required standards, listed below, that apply to all CEs. The addressable standards exist because of the range of organizational size and complexity of information management methods. In general, more effort and security technology is required of large organizations with many information sources and technologies than is required of small organizations. But the name addressable is somewhat of a misnomer in that all CEs that create, store, use or disclose e-PHI must document that they have considered every addressable standard and made a decision to implement it as prescribed by the rule, have created a functionally equivalent alternative approach, or document why the standard does not apply to their organization.

Requirements of the Rule fall into three general categories:

- **Administrative safeguards** focus on the security management process - the policies and procedures designed to prevent, detect, contain, and correct security violations. Required elements include:
    1. Performing and documenting a risk analysis (described below)
    2. Creating and maintaining a risk management plan
    3. Creating a sanctions policy
    4. Performing an information systems activity review
    5. Developing a security incident response and reporting mechanism

6. Creating a data backup plan
7. Creating a disaster recovery plan
8. Defining emergency mode operations
9. Having periodic evaluations of standards compliance

- **Physical safeguards** deal with facility access controls, standard workstation use and security, and device and media controls to protect ePHI from unauthorized disclosure, modification, or destruction. Required elements include:
    1. Workstation use analysis
    2. Mechanisms for physical workstation security
    3. Methods for disposal of media such as floppy disks, CDs, and tapes
    4. Methods to delete PHI prior to re-use of media

- **Technical safeguards** are policies and procedures for access control on systems that maintain ePHI. Required elements include:
    1. Unique User Identification
    2. Emergency Access Procedures
    3. Audit controls (i.e., logs of who created, edited or viewed ePHI)
    4. Authentication procedures (e.g., unique user ID and password for all users)

These 17 required elements are accompanied by 17 addressable elements that are beyond the scope of this document. See the full text of the Rule[2] for additional information on the addressable elements.

Implementing the Security Rule

CEs that create, use or disclose ePHI must designate a Security Officer who has responsibility for implementing HIPAA-compliant policies and procedures for use of e-PHI. The Security Officer and the group within the organization responsible for compliance must:

- Do and document a risk analysis that includes:
    - An Inventory of all sources of e-PHI
    - A Listing of who has access, when and where (including access from home or other locations outside of the CE's facilities)
    - An outline of the flow of e-PHI
    - A listing of storage locations and capacities
    - A listing of current security measures
    - An Analysis of potential confidentiality breaches
- Create a risk management plan based on the risk analysis
- Create and keep current a HIPAA Security Rule compliance document that includes description of how the 17 required elements are met, and decisions regarding Addressable elements

Biomedical Research and the Security Rule

As noted above, there is considerable effort, cost and complexity involved in compliance with the Security Rule. Although the Privacy and Security Rules were created to address healthcare services, they may have substantial impacts on biomedical research. In most academic health centers, management of information technologies for clinical systems is done centrally, by an Information Systems group or department. In contrast, most research data is maintained locally by investigators using a variety of technologies that range from Personal Digital Assistants and laptop computers to multi-user shared data repositories. The use of personal workstations running simple single-user database or spreadsheet programs is common in research settings. Compliance with the Security Rule for these types of systems may be problematic and economically unfeasible.

A key issue with respect to the Security Rule is how the how the organization has defined the functions included within its Covered Entity. As noted in the text of the Rule:

> Researchers who are members of a covered entity's work force may be covered by the security standards as part of the covered entity. *See* the definition of ''workforce'' at 45 CFR 160.103. Note, however, that a covered entity could, under appropriate circumstances, exclude a researcher or research division from its health care component or components (*see* § 164.105(a)). Researchers who are not part of the covered entity's workforce and are not themselves covered entities are not subject to the standards.[3]

If research is not part of the CE then any researcher access of PHI becomes a "disclosure" requiring an accounting and either authorization or waiver of authorization by an Institutional Review Board or Privacy Board. Although it may seem counterintuitive that movement of PHI inside of an organization is a disclosure, a potential benefit is that subsequent management of that information in electronic form is subject to best practices for maintaining of confidentiality, but is not subject to HIPAA Security Rule requirements since it is no longer within the CE. The University of California (UC), for example, established a systemwide Hybrid Covered Entity that includes health care components of the University but excludes education and research components. The UC HIPAA Task Force also created the concept of Research-related Health Information (RHI) to describe research uses of person-identifiable health data not arising out of a healthcare service event.[4]

Institutions that include research within the CE realize the benefit that research uses of ePHI may be considered a "use" rather than a "disclosure" which may reduce the accounting burden, but the Security Rule then potentially applies to any research computer application that includes an element of PHI (e.g., an Excel spreadsheet where one of the columns is a medical record number or date of hospital admission).

Defining "Covered" Research

AAMC member institutions have chosen a variety of different approaches to defining what areas of research should be covered by HIPAA and therefore require security

protections. The following are three possible options.

1. Organizational Unit Method: This method includes specified organizational units in the health sciences, such as the Schools of Medicine, Nursing, Dental and Public Health.

2. Clinical vs. Basic Science Method: This method designates individual faculty or specific labs as being part of the covered entity, e.g. including clinical faculty and excluding basic science faculty.

3. Project Method: A third option is to consider whether or not HIPAA applies on a "per project" basis. An example would be including research that involves the provision of health care in the CE and declaring that research that does not include the provision of health care is outside of the CE. Another method would be to include research that either creates or accesses PHI. In this regard, the federal Office of Civil Rights has provided specific guidance that if a study involves the delivery of routine health care and involves access to person-identifiable health data, and then the project is subject to the HIPAA Privacy and Security Rules.

Research Practices That Don't Meet the Standard

When a research project does involve ePHI, there will be a number of issues to confront. As a practical matter, many biomedical research workgroups have no written security procedures, policies or training. Conducting a risk analysis and creating a risk mitigation plan is not within the usual skill set of life sciences researchers. Information technology groups that possess this expertise have limited resources to provide this type of service to the dozens or even hundreds of researchers who typically work within academic medical centers. And databases containing ePHI that was or is being collected for unspecified research need to be identified and their HIPAA compliance addressed, since unlike the Privacy Rule, the Security has no grandfather provision for data already collected.

In addition, some widely used computer technologies are not compliant with the Security Rule. Examples include workstations with no login security (e.g., Windows98) and data management and analysis applications used to store PHI that have no ability to generate audit trails. A common example would be use of Excel spreadsheets containing ePHI in one or more columns, for which there is no technical capability to generate an audit trail, which is one of the required Technical Safeguards.

Minimizing the impact of the HIPAA Security Rule

To reduce the impact on biomedical research of the Security Rule, researchers should use either De-identified data and/or Limited Data Sets wherever possible, as defined by the HIPAA Privacy Rule. This will limit the need for disclosure accounting and permit the use of desktop computer applications that are not capable of being made compliant with the Security Rule. A bitter irony of the Security Rule is that it is likely to cause some

researchers to store PHI only on paper, where it becomes ineffective for support of automated clinical research protocol management utilities such as appointment reminder systems, and becomes an additional source of liability with respect to unintentional loss and disclosure.

Summary

Decisions made by academic health centers for purposes of complying with the HIPAA Privacy Rule in 2003 will have profound impacts on compliance with the HIPAA Security Rule in beginning in 2005. From a policy perspective, the exclusion of research from the CE, as permitted by the Security Rule, appears to be the single most important approach to minimizing the costs and legal liabilities of the Security Rule.

---

[1] Information regarding the HIPAA Privacy and Security Rules is available online at http://www.hhs.gov/ocr/hipaa/

[2] Full text of the Security Rule is available online at http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp

[3] 45 CFR Part 142, as published in Federal Register, Vol. 68, No. 34, Feb 20, 2003 p. 8338

[4] http://irb.ucsd.edu/WhatIsandIsNotPHI.pdf