Reframing the Influence of the Health Insurance Portability and Accountability Act on Research

Carol Bova, PhD; Deborah Drexler, JD; and Susan Sullivan-Bolyai, DNSc

The purpose of this article is to review the Health Insurance Portability and Accountability Act (HIPAA), the Privacy Rule, the Security Rule, and common issues encountered by researchers related to these federal privacy and security requirements. This article discusses the misconceptions that researchers may hold about HIPAA, including the process for reviewing protected health information when preparing to conduct a study, potential constraint on participant recruitment, and application of HIPAA to a researcher's clinical population. We also present ways to reframe the negative connotations associated with this regulation and provide tips for researchers about how to work with HIPAA when planning and conducting a study and reporting on study findings. Finally, we suggest that the principles of HIPAA be considered when conducting studies in international settings.

CHEST 2012; 141(3):782–786

Abbreviations: HIPAA = Health Insurance Portability and Accountability Act; IRB = institutional review board; PHI = protected health information

How many times have we read about the negative influence of the Health Insurance Portability and Accountability Act (HIPAA) on the research enterprise? Reports suggest that HIPAA compliance places an added burden on institutional review boards (IRBs), researchers, and human subjects.^{1–3} Words such as “nuisance,” “costly,” and “ineffective” have been used to describe the effect of the HIPAA on research. It is true that in the pre-HIPAA era, researchers could easily access patients and patient information directly. Previously, researchers had free rein to recruit subjects in clinic waiting rooms, as they entered EDs, and in their hospital beds. Researchers were also able to obtain lists of potential research

subjects from patient clinical rosters. Therefore, recruitment was easier. Health-record-based research was facile. There was less paperwork and fewer forms to develop, submit, and have approved. There was less time spent on research compliance training. However, the question arises: Is easier always better?

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA (Public Law 104-191) was enacted on August 21, 1996. The purpose of this act was to help reform the health insurance industry and to streamline health-care administrative processes. This act authorized the secretary of Health and Human Services to inform the public about the standards for privacy, electronic exchange, and security of patient health information. After a lengthy public debate and much controversy, the Standards for Privacy of Individually Identifiable Health Information (known as the Privacy Rule) became effective in April 2003. Goals of the Privacy Rule were twofold: (1) to allow for the electronic flow of health information between covered entities (health plans, health-care providers, health-care facilities, health-care clearinghouses)

Manuscript received August 29, 2011; revision accepted October 10, 2011.

Affiliations: From the Graduate School of Nursing (Drs Bova and Sullivan-Bolyai), and the Center for Health Care Financing (Ms Drexler), University of Massachusetts Medical School, Worcester, MA.

Correspondence to: Carol Bova, PhD, University of Massachusetts Medical School, Graduate School of Nursing, 55 Lake Ave N, Worcester, MA 01655; e-mail: carol.bova@umassmed.edu

© 2012 American College of Chest Physicians. Reproduction of this article is prohibited without written permission from the American College of Chest Physicians (<http://www.chestpubs.org/site/misc/reprints.xhtml>).

DOI: 10.1378/chest.11-2182

with the purpose of promoting high-quality health care; and (2) to protect the public's health and well-being and the privacy of patient health information (see <http://www.hhs.gov/ocr/hipaa>). The Standards for the Protection of Electronic Protected Health Information (also known as the Security Rule) became effective in 2005 to further operationalize the mandates in the Privacy Rule pertaining to the security of electronic health information.¹ The Security Rule requires that covered entities take appropriate steps to protect the confidentiality, integrity, and availability of all electronic protected health information (PHI) that they create, receive, maintain, or transmit; protect against reasonable breaches or disclosure of PHI; and train their workforce in data security compliance. Such appropriate steps include the technical (eg, user password procedures, auditing of data access), the physical (eg, deletion of PHI, disposal of data stored electronically, personal computer security), and the administrative (eg, risk-management processes and sanctions) security of electronic data. Today, the federal Office of Civil Rights is responsible for enforcing the HIPAA Privacy Rule and the HIPAA Security Rule.

HIPAA AND THE COMMON RULE

The overall goal of the Privacy and Security Rules is to protect PHI at a time when electronic transfer of health data is becoming the norm. Significantly, these rules had an indirect role in regulating human subject participation in research. Prior to the rules, the Common Rule was the mainstay of research regulation. The Common Rule, published in 1991, specifies requirements for IRBs, for informed consent processes, and for research in vulnerable populations (eg, pregnant women, fetuses, prisoners, and children).

The Common Rule applies to research that receives funding from any of 17 federal agencies. However, institutions with a Federalwide Assurance agree to comply with the Common Rule requirements regardless of funding source (this includes internally funded research, international research, and collaborative research across institutions). As a practical matter, all research conducted by academic medical centers in the United States must comply with the Common Rule.

Health and Human Services recently announced (July 2011) plans to improve and strengthen the Common Rule by examining the level of review required based on the level of risk, updating informed consent processes, considering single IRB review for multi-site studies, establishing mandatory data security procedures, harmonizing adverse event reporting, and extending the reach of federal regulations to protect

human research subjects. It is too soon to tell how the requirements of the HIPAA Privacy and Security Rules will be integrated into the revised Common Rule.

WORKING WITH HIPAA'S PRIVACY AND SECURITY REQUIREMENTS

In practice, the HIPAA rules limit the ability of a researcher to access PHI without following certain requirements. The general rule is that covered entities must obtain written permission, known as an "HIPAA authorization," from each patient before the covered entity can release the information to an outside researcher or use the patient's information internally for research purposes. In situations in which obtaining an authorization is impractical or impossible, a major exception to the general rule allows a researcher to request from an IRB a "waiver of authorization," which allows a covered entity to use or disclose data for specified research purposes without such an authorization.

Besides this general rule and its major exception, the HIPAA Privacy Rule established two more processes about which researchers should know. First, recognizing that researchers may need access to PHI before research even begins, to establish whether a research study is feasible, the Privacy Rule created a process allowing a covered entity to use or disclose PHI for a "review preparatory to research." Under this process, a researcher may freely review PHI to determine whether a research study is feasible but may not use that PHI for any other purpose at that time and may not remove that PHI from the covered entity's premises. The Privacy Rule also allows a covered entity to use or disclose a set of "partially deidentified data" (known as a "limited data set") for research purposes without obtaining either an authorization or a waiver of authorization. Limited data sets do not contain names, addresses, or other direct identifiers but may contain zip codes, towns of residences, and dates of birth and service. Of course, a completely deidentified data set, one stripped of all 19 identifiers listed in the Privacy Rule, is not subject to the rules' requirements at all. See Table 1 for a list of the identifiers.

The HIPAA Security Rule is also important to consider because it governs the storage of electronic PHI and the transfer of electronic PHI from one location to another, both considerations frequently encountered in contemporary research practice. (Note: The Security Rule pertains to electronic PHI only.) Individual institutions have various administrative safeguards put in place to secure electronic data used for clinical and research purposes. Much of this work takes place at an organizational level, but it is essential that

**Table 1—HIPAA: Protected Health Information
List of Identifiers**

A de-identified data set is one that does not include any of the following

1. Patient names
2. Geographic subdivisions smaller than a state (street, city, county, zip code, geocodes)
3. Dates (birth date, admission date, discharge date, date of death)
4. Age > 89 y (unless data are reported in a single category of age ≥ 90 y)
5. Phone numbers
6. Fax numbers
7. E-mail addresses
8. Social Security numbers
9. Medical record numbers
10. Health plan beneficiary numbers
11. Account numbers
12. Certificate or license numbers
13. Vehicle identifiers (serial numbers, license plate numbers)
14. Device identifiers and serial numbers
15. Web Universal Resource Locators (URLs)
16. Internet Protocol (IP) addresses
17. Biometric identifiers (including fingerprints and voiceprints)
18. Full-face photographic images
19. Any other unique identifying number characteristics or codes that could be linked back to an individual (this does not include a unique research identification code)

A limited data set is one that may contain zip codes, towns of residence, or specific dates, but no other identifiers listed above. Listed identifiers have the potential to link data to an individual patient. HIPAA = Health Insurance Portability and Accountability Act.

individual researchers be aware of the rules and regulations governing securing and transferring electronic data within and across institutions. For example, the use of outdated software that does not require a security login or the use of Excel spreadsheets that do not provide for audit trails of stored electronic PHI would likely violate the Security Rule.⁴ Virtually all research institutions now prohibit the use of software that violates this rule.

It may appear that HIPAA principles are quite simple. However, one of the problems is that the HIPAA language is open to many interpretations. Therefore, institutions often interpret these principles differently, causing inconsistency in the way the Privacy Rule is applied in various research settings. Therefore, the first step is for researchers to find out how their institution interprets these rules and to become familiar with how their IRB handles HIPAA authorizations, waiver of authorization, disclosure of limited data sets, and deidentified data. It is also important to understand that the HIPAA Privacy Rule may not be as stringent in protecting PHI as are state laws, in which case the state laws take precedence.

Next, it is important to think about HIPAA issues during the initial planning stages of any study. Many researchers wait and think about HIPAA only after a proposal is written and they are in the process of sub-

mitting their application to an IRB. Considering the need for HIPAA authorization at the onset of study development prevents researchers from getting too far into the planning phase only to find out that there may be some data access issues that were not considered. Planning for HIPAA will decrease researcher frustration and prevent delays.

It is important to clarify several common misconceptions that researchers often hold about HIPAA, including that (1) researchers are unable to review PHI when preparing to do a study, (2) HIPAA rules constrain recruitment opportunities, and (3) HIPAA rules do not apply to a researcher's clinical population. Under the "review preparatory to research" provisions of the Privacy Rule, researchers are allowed to review a covered entity's PHI when determining whether a study is feasible. This type of review might be useful, for example, when the researcher needs to find out how many potential research subjects are in the accessible population (including how many will meet specific inclusion/exclusion criteria). Some institutions require researchers to obtain an HIPAA waiver before accessing PHI in preparation for conducting a study, but this is not required by the Privacy Rule.

Nothing in the HIPAA Privacy Rule explicitly changes research recruitment procedures, but it does require generally that a covered entity obtain an HIPAA authorization allowing the release of its PHI to a researcher before patients are approached to be in a study. Some have suggested that this additional step is burdensome for patients and that patients are less likely to participate in a study if they have to sign an HIPAA authorization.⁵ But it is important to consider that the HIPAA provides potential research participants with the details of what PHI will be disclosed to the researcher and how the PHI will be used. It is possible that a greater number of people will decide that they do not want their PHI to be used or disclosed in this manner. Thus, the HIPAA actually adds to the entire process of obtaining fully informed consent by detailing, at the onset, exactly what data will be released to researchers even before a patient is recruited for a specific study.

Finally, it is important to recognize that many researchers are also clinicians with active medical practices. These clinicians must still comply with the Privacy Rules when recruiting research subjects from their own patient population. Clinicians often argue that they review PHI for clinical purposes, such as to evaluate how well they are doing in managing a particular condition or performing according to practice guidelines. However, when clinicians use their patients' PHI for the purpose of generating a pool of patients to recruit for a study, for generating hypotheses, or for any other research purpose, they

are functioning as researchers and must comply with all the research provisions of the HIPAA rules.

When conducting research in international settings, there is considerable debate and variable practice about whether and how the HIPAA Privacy and Security rules apply. Some US institutions do not apply HIPAA principles to research wholly conducted outside the United States, although many institutions believe that once a US covered entity collects identifiable health information, that information becomes PHI and covered by the Privacy and Security Rules. Unfortunately, the concept of HIPAA authorization is often difficult to explain to researchers in resource-limited settings. Once again, it is crucial for researchers to understand exactly how their sponsoring institution handles these situations. Some institutions encourage researchers to include simplified HIPAA authorization language within the informed consent document, or, for low-risk studies, to obtain verbal consent to collect and transfer PHI. Some settings advise researchers to request a waiver of HIPAA authorization from their IRB to allow an independent judgment to take place about the applicability of HIPAA to the international setting. In addition, researchers need to review the laws, regulations, guidelines, and common practices in use in specific countries, some of which may be stricter than the HIPAA rules. An excellent resource for investigators is the document produced yearly by the Office for Human Research Protections, entitled *International Compilation of Human Research Protections*, which lists the human subjects' requirements for more than 101 countries (available at <http://www.hhs.gov/ohrp/international/intlcompilation/hspcompilation-v20101130.pdf>). Note that most researchers agree that the Common Rule applies to international work done by US researchers. We suggest that the principles of HIPAA not be limited to studies done in the United States but be considered integral to conducting research in international settings. Hopefully, the Common Rule revisions will provide greater guidance on how to integrate privacy, security, and humans subjects' protection within international settings. Table 2 contains information that will help researchers apply HIPAA principles as they plan, conduct, and report the results of research studies.

CONCLUSION

In sum, HIPAA is here to stay. PHI is more accessible than ever and extra protection of these data is needed as we rely more on electronic medical records, data repositories, and electronic transfer of data. Researchers need to reframe the negative connotation often associated with HIPAA (eg, obstructionism,

Table 2—Tips for Making HIPAA Work for You

1. Consider HIPAA requirements as you plan your study (avoid waiting until the end)
 - a. Be familiar with your institution's HIPAA policies (authorization, waiver, data use agreements, limited data sets, international research requirements) and those of any other planned research sites.
 - b. Take advantage of HIPAA training and data security updates at your institution (encourage members of your research team to attend these sessions also).
 - c. Make sure your research team is adequately trained about HIPAA.
 - d. Avoid collecting PHI that is not needed.
 - e. When conducting research in international settings, be aware that following HIPAA requirements provides added protection for human subjects and should be used in any human subject research.
2. Consider HIPAA requirements as you carry out your study
 - a. Use encryption when transferring data over the Internet and storing research data on portable computers or devices.
 - b. Keep identifying data separate from research data.
 - c. Limit access to PHI.
 - d. Deidentify data as soon as direct identifiers are no longer needed.
 - e. Remember that if you need to rework your recruitment plan, you may need to apply for an HIPAA waiver or additional HIPAA authorization.
3. Consider HIPAA requirements when you present your study findings
 - a. Make sure to keep your results anonymous. This can be a particular concern when data are collected using very small sample sizes (such as in feasibility studies) or from patients with rare conditions. It is also a major concern for reporting qualitative data (including interview and focus group data).
 - b. Remember to double-check all attached materials to ensure that any PHI has been removed from them. Keep in mind that identifiers are commonly included by default on radiology films and other diagnostic images; some systems have a mechanism in place to automatically eliminate these identifiers, whereas in other cases you may need to remove them manually.
 - c. Make sure to indicate how you met the HIPAA requirements for accessing your sample and/or collecting PHI (this applies to preparing abstracts, posters for conference presentations, and manuscripts).

PHI = protected health information. See Table 1 for expansion of other abbreviations.

time consuming, needless, and not effective) to a positive one that appreciates the idea that each patient has the right to know when PHI is being used for research purposes. Participation in a research study is an act of generosity and altruism on the part of the human subject and is a personal choice, not a mandate. Thus, the HIPAA provides potential study subjects' additional privacy protection prior to recruitment. These days, when information security breaches are common, the HIPAA provides an extra layer of protection for our patients and their families. It should be considered another transparent check and balance that is part of the scientific integrity process on the forefront of prestudy development

and planning. Thus, it is best to understand the benefits of the HIPAA and how to work with the rules, rather than resist them. We owe this to our patients and our research participants.

ACKNOWLEDGMENTS

Financial/nonfinancial disclosures: The authors have reported to *CHEST* that no potential conflicts of interest exist with any companies/organizations whose products or services may be discussed in this article.

REFERENCES

1. Ness RB; Joint Policy Committee, Societies of Epidemiology. Influence of the HIPAA Privacy Rule on health research. *JAMA*. 2007;298(18):2164-2170.
2. Infectious Diseases Society of America. Grinding to a halt: the effects of the increasing regulatory burden on research and quality improvement efforts. *Clin Infect Dis*. 2009;49(3):328-335.
3. Wartenberg D, Thompson WD. Privacy versus public health: the impact of current confidentiality rules. *Am J Public Health*. 2010;100(3):407-412.
4. Masys, D. Research and the HIPAA Security Rule. Paper prepared for the Association of American Medical Colleges. University of Miami Miller School of Medicine Web site. <http://www.med.miami.edu/hipaa/public/documents/researchsecurityrule.pdf>. March 8, 2005. Accessed August 6, 2011.
5. Beebe TJ, Talley NJ, Camilleri M, Jenkins SM, Anderson KJ, Locke GR III. The HIPAA authorization form and effects on survey response rates, nonresponse bias, and data quality: a randomized community study. *Med Care*. 2007;45(10):959-965.