VIReC

VIReC Insights is intended to provide VA researchers with a starting point for understanding concepts in data management and basic information about health related databases.

Upcoming Issue:

VA Medicare Data for Research

Vol. 4 | Number 3 | Winter 2003

VA INFORMATION RESOURCE CENTER
EDWARD HINES JR. VA HOSPITAL
PO BOX 5000 (151V)
HINES, ILLINOIS 60141
PHONE: (708) 202 2413
FAX: (708) 202 2415
VIREC@RESEARCH.HINES.MED.VA.GOV
WWW.VIREC.RESEARCH.MED.VA.GOV

INSIGHTS

Vol. 4 | Number 2 | Summer 2003

Research Implications of the Privacy Standards Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Patricia L. Watts, J.D., Denise M. Hynes, Ph.D., and April Kopp

Introduction

In this issue of *VIReC Insights*, we provide a brief background of HIPAA, describe the Privacy Rule, and review the VHA research implications while highlighting and defining key terms and relevance to the research process. We conclude with specific references and Web citations for additional information.

Background

The purpose of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191) is to improve portability and continuity of health insurance coverage in the group and individual markets. A key element in accomplishing this objective is the simplification of the administration of health insurance. The Administrative Simplification provision of the law included five focus areas: transactions, code sets, identifiers, security, and privacy. The Department of Health and Human Services (DHHS) has the rule-making authority for these five areas.

The Standards for Privacy of Individually Identifiable Health Information (45 CFR parts 160 and 164), commonly known as the HIPAA Privacy Rule, were published in final form in December of 2000, and amended in May and August of 2002. The compliance date for the Privacy Rule was April 14, 2003.

The Privacy Rule directly addresses the patient's concern for protection of personal information. Moreover, HIPAA results from recognition of certain evident factors in health care, such as the increase of the number of organizations involved in the provision of care and processing of claims, the growing use of electronic information technology, increased efforts to market health care and other products to consumers, and the increasing ability to collect highly sensitive information about an individual's current and future health status as a result of advances in scientific research. The HIPAA Privacy Rule establishes, for the first time, a set of basic national privacy practices that provide all Americans with a fundamental level of protection, including parameters for research uses of protected health information.

There are some unique implications of the Privacy Rule in VHA.* In the next section, we highlight key terms and areas researchers need to understand about HIPAA in conducting research in the VA.

* The Office of Research and Development issued guidance on implementation of the Privacy Rule on April 4, 2003 (Memorandum, available at: http://www.va.gov/resdev/fr/HIPAAMemo040403.doc).

Top Ten Things VHA Researchers Should Know About the HIPAA Privacy Rule

1. VHA is a single covered entity for purposes of the Privacy Rule.

VHA is one of several federal healthcare programs named in HIPAA as a covered entity. Because of this provision and because of the logistics of the VHA system, VHA officials determined that it was appropriate to treat the entire system—all hospitals, doctors, clinics, etc.—as a single covered entity, rather than a series of individual covered entities. For researchers, this means that they are part of a covered entity rather than external to the covered entity—a distinction that does make a difference in access to information.

2. Research conducted within VHA is a USE, not a DISCLOSURE.

The Privacy Rule defines use as "the sharing, employment, application, utilization, examination, or analysis of such information **within** an entity" that maintains individually identifiable information. Disclosure is defined as "the release, transfer, provision of, access to, or divulging in any other manner of information **outside** the entity holding the information" (National Institutes of Health 20).

VHA research, because it is conducted **within** the covered entity, is a **use** of PHI, rather than a disclosure. This distinction has several implications:

- The Privacy Rule requires that all DISCLOSURES be accounted for as long as six years. This provision does not apply to USES of information, however, so research conducted solely within VHA is not subject to the accounting provision.
- Because VHA is a single covered entity, even research requiring data collected from several VHA sites will be a use, not a disclosure. So a researcher at a VHA facility in California may "use" information from a VHA facility in Illinois without triggering any of the disclosure provisions in the Privacy Rule. However, each facility still maintains control of its own information and may require a researcher to comply with its information practices.

3. The HIPAA Privacy Rule does not change the Common Rule.

In general, all federally funded research is conducted under the provisions of the Federal Policy for the Protection of Human Subjects in Research, known as the "Common Rule." Although some research may be determined to be "exempt" from the Common Rule, such exemption does not provide similar exemption from the mandates of the Privacy Rule. The Privacy Rule specifically applies to the protection of personal information whereas the Common Rule applies to the protection of human subjects in research. Also, the Privacy Rule does not weaken the authority of Institutional Review Boards (IRB) in approving research. In fact, it may necessitate that the IRB (in the absence of a Privacy Board) address privacy issues in their review of research protocols.

4. VHA Policy may conflict with Affiliate Policy.

Some VHA facilities have designated the IRB of an affiliated academic institution as the IRB of record for research. It is important to recognize that VHA policy, in implementing the Privacy Rule, may differ from that of the academic affiliate. VHA is a federal program, subject to the constraints of federal law that may not apply to state-based academic institutions. It is important, therefore, that a facility using the IRB of an academic affiliate work closely to educate the affiliate in the policies of the VHA. Use of an academic affiliate's IRB does not absolve the researcher from complying with federal laws. Researchers with dual appointments must understand each system and comply with the policies and procedures of each.

VA researchers should note also that VA policy may differ from external interpretation of the Privacy Rule. For example, NIH may not have the same interpretation as VA.

Key Terms to Know

AUTHORIZATION - Permission from a patient to use or disclose his/her information in a way not expressly permitted by the Privacy Rule. May be "waived" by IRB under certain conditions. (See Table 2)

COVERED ENTITIES - Those entities directly regulated by the Privacy Rule; generally includes doctors, hospitals, and insurance companies. Researchers are generally not covered entities, but VHA researchers are part of the covered entity.

PROTECTED HEALTH INFORMATION (PHI) - A subset of individually identifiable health information, the use or disclosure of which is regulated by the Privacy Rule. Eighteen (18) elements of PHI are clearly set forth in the Rule.

5. The Privacy Rule does not distinguish between types of research.

The Privacy Rule is intended to regulate the use and disclosure of information in and by a covered entity. Research is recognized as one reason a covered entity may use or disclose PHI. However, the provisions of the Privacy Rule for research do not distinguish between the types of research. A covered entity must determine how the Privacy Rule should apply to a proposed research study. For example, the requirement to obtain an Authorization from each subject may be appropriate in a clinical research study, while a Waiver of Authorization is more likely to be used in a retrospective chart review study.

Researchers should be familiar with the provisions of the Privacy Rule to be ready to answer questions from the IRB and to assist the IRB in determining the appropriate application for their study.

6. Creation of a database for research IS research.

Although the Privacy Rule is careful not to regulate research, per se, it does make clear that certain activities are considered research for purposes of the Rule and therefore subject to the applicable provisions. A key example of this is found in the Preamble to the August 2002 amendments to the Rule: "Under the Common Rule, OHRP has interpreted the definition of 'research' to include the development of repository or database for future research purposes… The Department interprets definition of 'research' in the Privacy Rule to be consistent with what is considered research under the Common Rule. Thus, the development of research repositories and databases for future research are considered research for purposes of the Privacy Rule" (67 *Federal Register* 53,231, August 14, 2002). To ensure compliance with the Privacy Rule, creation of a database for research is and will be treated as research. The research involves creation of a database of PHI, the research requires either an Authorization from the subjects or a Waiver of Authorization from the IRB.

7. Study sponsors generally are not business associates.

Clinical investigators had an additional concern under the Privacy Rule regarding whether a sponsor of their research, for example, a pharmaceutical company, was a "business associate" for purposes of the Privacy Rule. A business associate is defined as a person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information, such as data analysis, claims processing or administration, utilization review, and quality assurance reviews, any other function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule, or any other service as defined in the Privacy Rule (45 CFR (160.103) (2002)). The key element in determining whether an external entity is a business associate is whether the entity is performing a function on behalf of the covered entity. Generally, sponsors do not perform any function on behalf of the covered entity. Additionally, sponsors may not need to receive PHI as a result of the study, but rather can be given de-identified information or a limited data set. Finally, if a sponsor does need to receive PHI, adding the sponsor to the authorization to be signed by the subjects to a clinical trial may provide a simple way of doing so. As part of the informed consent process, subjects should be advised of this disclosure of their information to an external party and what the sponsor will do with the information.

8. Researchers can use De-identified Data, Limited Data Sets, and Data Use Agreements.

In earlier versions of the Privacy Rule, the only allowable use or disclosure of information for research required either an authorization signed by the subject or the use of "de-identified" data. Historically, some research has been conducted using "anonymized" data; that is, key elements of identification such as name and social security number were removed from a set of data. The Privacy Rule does not recognize the term "anonymized" but refers instead to "de-identified" data, which is defined as data that is stripped of eighteen elements (see Table 1). De-identification is far more stringent than anonymizing data as researchers have done for years. Because the research community argued that this new "de-identification" would seriously impair the ability to conduct research and link databases across multiple sources, DHHS included a compromise in the August 2002 amendments.

The compromise came in the form of a "limited data set" that contained more information useful to researchers than the strict de-identification provisions. Like de-identified data, a limited data set is defined by what is NOT in it. The Privacy Rule requires the elimination of sixteen identifiers to create a limited data set (see Table 1). While many of the elements

TABLE 1. Elements Excluded from De-Identified Data Set vs. a Limited Data Set

De-Identified Information excludes:	**Limited Data Set excludes:**
Names	Names
All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geographical codes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: a. The geographic unit formed by combined all zip codes with the same three initial digits contains more than 20,000 people b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000	Street address
All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older	
Telephone numbers	Telephone numbers
Facsimile (fax) numbers	Facsimile (fax) numbers
Electronic mail addresses	Electronic mail addresses
Social security numbers	Social security numbers
Medical record numbers	Medical record numbers
Health plan beneficiary numbers	Health plan beneficiary numbers
Account numbers	Account numbers
Certificate/license numbers	Certificate/license numbers
Vehicle identifiers and serial numbers, including license plate numbers	Vehicle identifiers and serial numbers, including license plate numbers
Device identifiers and serial numbers	Device identifiers and serial numbers
Web universal resource locators (URLs)	Web universal resource locators (URLs)
Internet protocol (IP) address numbers	Internet protocol (IP) address numbers
Biometric identifiers, including fingerprints and voiceprints	Biometric identifiers, including fingerprints and voiceprints
Full-face photographic images and any comparable images	Full-face photographic images and any comparable images
Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification	

are the same as those required to be removed for de-identification, several subtle differences make a limited data set more valuable to a researcher. For example, de-identification requires eliminating all geographic information smaller than a state while a limited data set can include any geographic code greater than postal (street) address. De-identified information cannot contain any elements of dates, other than year, that pertain to the individual, but a limited data set may have full dates within it (45 CFR (164.514(e)(2)) (2002)).

The caveat on using a limited data set is that it requires the use of a data use agreement. Data use agreements (DUAs) are not new; they have been employed by data brokers long before the advent of HIPAA. The DUA is exactly what it says: an agreement to use data in the ways spelled out in the document. The Privacy Rule contains explicit provisions that must be contained in a DUA accompanying a limited data set (45 CFR (164.514(e)(4)) (2002)).

VHA Handbook 1605.1, Privacy and Release of Information, states that **within** VHA, researchers do not need to use a DUA. This does not prohibit the use of the DUAs by groups that wish to add that layer of protection when sharing information with other researchers inside the VHA. For example, if a researcher asks for information from a VHA data registry, the registry may require the researcher to sign a DUA that clearly states the researcher's obligations for protecting the data and the ways in which the data could be used.

A researcher should not release identifiable data **outside** the VHA, even in a limited data set, without checking with the privacy officials at their site or at Central Office. This does not apply if an authorization has been signed by the

TABLE 2. Requirements for a Valid Authorization, according to the Privacy Rule

Core Elements	
1	Description of the PHI to be used or disclosed, identifying the information in a specific and meaningful manner
2	The names or other specific identification of the person or persons (or class of persons) authorized to make the requested use or disclosure
3	The names or other specific information of the person, persons, or class of persons authorized to receive the information
4	A description of each purpose of the requested use or disclosure
5	Authorization expiration date or expiration event that relates to the individual or to the purpose of the use or disclosure ("end of the research study" or "none" are permissible for research, including for the creation and maintenance of a research database or repository)
6	Signature of the individual and date. If the individual's legally authorized representative signs the Authorization, a de scription of the representative's authority to act for the individual must also be provided
Required Statements	
1	A statement of the individual's right to revoke his/her Authorization and how to do so, and, if applicable, the exceptions to the right to revoke his/her Authorization or reference to the covered entity's notice of privacy practices, if the exception information is contained there
2	Whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on Authorization, including research-related treatment and consequences of refusing to sign the Authorization, if applicable
3	A statement of the potential risk that PHI will be re-disclosed by the recipient and no longer protected under HIPAA
Additional Procedures	
1	A signed copy given to the individual
2	The Authorization written in plain language

TABLE 3. Required Documentation for Alteration or Waiver of Authorization

Required Elements
The IRB must determine that a request for a Waiver of Authorization satisfies **all** the following criteria:
1. Identification of IRB
2. Date of IRB approval or Waiver of Authorization

3. Alteration or Waiver of Authorization criteria:
• Use/disclosure involves no more than minimal risk to the privacy of individuals based on, at least, the presence of:
  • An adequate plan to protect identifiers from improper use and disclosure
  • An adequate plan to destroy identifiers at earliest opportunity unless health or research justification or required by law
  • Adequate written assurances
• That the research could not practicably be conducted without waiver or alteration
• Research could not practicably be conducted without access to and use of PHI

4. Description of PHI needed
5. Identification of the review procedure used to approve the Waiver of Authorization
6. Signature of the chair of the IRB or member designated by the chair to approve the Waiver of Authorization

patient or a waiver of authorization has been granted by the IRB (see below). The Office of Research and Development is working with the Privacy Office of VHA to develop standards for limited data sets and data use agreements that can be used by researchers.

9. Only research may use Waivers or Alterations of Authorization.

Often, research projects require more information than can be obtained from a limited data set or de-identified data. Sometimes the number of subjects or records being reviewed is too vast for signed Authorization (see Table 2) to be obtained from every individual subject. The Privacy Rule addresses these exceptions through criteria for Waivers or Alterations of Authorization (see Table 3) by an IRB or a Privacy Board (45 CFR (164.512(i)(1) and (2)) (2002)). The covered entity, acting through the IRB, must determine that the circumstances warrant the use of a Waiver or Alteration.

A Privacy Board is an entity identified in the Privacy Rule as an alternative to an IRB for Privacy Rule purposes. A covered entity is not required to create a Privacy Board if it currently has an IRB that will perform the functions required. to grant Waivers or Alterations of the Authorization. Currently, all VHA facilities are using IRBs to perform these functions.

It is important to note that research is the only activity for which a Waiver or Alteration is allowable. Any other activity not specifically allowable under the Privacy Rule requires the Authorization of the individual to whom the information pertains.

10. Penalties for violating the Privacy Rule are steep.

The penalties for violating the Privacy Rule are contained in the statute, rather than in the Rule itself. They include both civil sanctions (42 USC 1320d–5) and criminal sanctions (42 USC 1320d–6).

Civil sanctions will be enforced by the Centers for Medicare and Medicaid Services (CMS) within DHHS. The sanctions imposed according to the statute are $100 per violation of any provision. The statute also allows for a maximum penalty of $25,000 per year. However, that is $25,000 "for all violations of an identical requirement or prohibition." So if the records of 250 patients are disclosed improperly, that is

$25,000 (250 x $100). But if that disclosure violates more than one provision of the Administrative Simplification provision, multiple penalties of $25,000 could be levied.

The civil sanctions are trumped by the criminal sanctions—the law does not allow civil penalties to be levied if criminal charges are filed. The criminal sanctions are severe and depend on whether the violator "knowingly":

- Uses or causes to be used a unique identifier,
- Obtains individually identifiable health information, or
- Discloses individually identifiably health information.

If the violation meets the above criteria, the allowable sanction is no more than $50,000 fine, or 1 year in prison, or both. However, if the offense includes "false pretenses," the fine rises to $100,000, or 5 years in prison, or both. Finally, if there is an "intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm," the violator can be fined up to $250,000, or 10 years in prison, or both. Criminal sanctions will be enforced by the Department of Justice.

Summary

This introduction to HIPAA privacy issues provides a starting point for researchers. VIReC will continue to address both privacy and data security implications of HIPAA. A manuscript is being developed for a peer-reviewed journal, and a panel presentation will be made at the 2003 QUERI Annual Meeting. Entitled *Data Resources, Privacy, and Security: Things You Need To Know,* the panel will focus on data sharing policy development, data security and exemptions, storage of data, and issues surrounding transmitting and receiving data. Please also see the information below in "Additional Resources."

References

National Institutes of Health. *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*. DHHS. NIH Publication Number 03-5388. Available at http://privacyruleandresearch.nih.gov/pr_02.asp.

Office for Civil Rights (OCR), DHHS. Standards for privacy of individually identifiable health information. Final rule. *Federal Register*. 2002 Aug 14;67(157):53181-273.

Office of Research and Development. HIPAA Guidance Document. Veterans Health Administration. 2003 Feb. Available at http://www.va.gov/resdev/fr/hipaa.cfm.

The Standards for Privacy of Individually Identifiable Health Information (45 *Code of Federal Regulations* Parts 160 and 164), as amended (2002).

United States Code (Title 42, Section 1320d–5 and 1320d–6) (2000).

Wray, NP. Memorandum: "HIPAA Privacy Rule Compliance Steps," April 4, 2003. ORD. Available at http://www.va.gov/resdev/fr/HIPAAMemo040403.doc.

Additional Resources

Federal Policy for Protection of Human Subjects in Research (Common Rule) codified for VA at 38 CFR Part 16.

DHHS OCR Web site. Medical Privacy - National Standards to Protect the Privacy of Personal Health Information (http://www.hhs.gov/ocr/hipaa/).

DHHS Office of Human Research Protections (OHRP) Web site. (For formal guidance on interpretation of HHS regulations at 45 CFR Part 46, Protection of Human Subjects, available at: http://ohrp.osophs.dhhs.gov).

DHHS Web site. HIPAA Privacy Rule: Information for Researchers (http://privacyruleandresearch.nih.gov).

Suggested Citiation:
Watts PL, Hynes DM, & Kopp A. Research Implications of the Privacy Standards Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). VIReC Insights Vol. 4, No. 2. Hines, IL: VA Information Resource Center, 2003. Available at http://virec.research.med.va.gov. Accessed [date].

RESEARCHERS' GUIDE TO VA DATA

VIReC Mission

To improve the quality of VA research that utlizes databases and information systems.

VIReC Insights is also published three times a year on the VIReC Web site. You can visit our website at:

www.virec.research.med.va.gov

Insights Staff

Editor-in-Chief: Denise M. Hynes, PhD
Managing Editor: Patricia A. Murphy, MS
Design / Layout: Cody Tilson
Production: Keisha Greenwood

RESEARCHERS' GUIDE TO VA DATA
EDWARD HINES JR. VA HOSPITAL
PO BOX 5000 (151V)
HINES, ILLINOIS 60141