HIPAA Research Tutorial

Health Insurance Portability and Accountability Act

Please review the material. Check the boxes once the content has been reviewed. Once all content has been covered please complete the form and upload it to your IRBNet User Profile utilizing the Training and Credentials tool.

HIPAA Overview

HIPAA is an acronym for Health Insurance Portability and Accountability Act. This federal law is best known for allowing individuals to maintain health insurance when they change employers. HIPAA establishes privacy standards in order to protect an individual's health information. This Act is designed to enable a person to go from one health insurance plan to another with continuity of care and not be denied coverage for a pre- existing condition (portability) and places protections for confidentiality of protected health information (PHI) that is collected (accountability). The privacy section of HIPAA, called the *Privacy Rule*, imposes restrictions on th 8 Td[(th 8us /84 (l)1(not 3.8 (odisclosund)158 (l)1.35 T6.5(H)1240(o)1I)5.15 Tc 0 Tw 131.6742 0 0 10.98 431.7

A covered entity (i.e., University of South Alabama)

research purposes. The hospital based training program pertains to health care, while the Office of Research Compliance and Assurance requires that all researchers and key personnel complete HIPAA training as it pertains to research reviewed by the IRB.

This tutorial satisfies the training requirement set forth by the Privacy Rule as it pertains to research that utilizes protected health information during the course of a study

What Constitutes Research Activities?

- Results are expected to be published or presented at a conference with attendees who are NOT

2) One of the following criteria must be met:

- IRB Waiver of Subject Authorization
- 0.0005 Tc09 Tw 2)

consent within the confidentiality section. Although the authorization can be separate from the informed consent document per the HIPAA regulations, the IRB has adopted that these documents be combined as it simplifies the procedure for authorization.

The core elements listed above must be provided in writing to prospective subjects in securing authorization for the research use of their PHI. The USA HIPAA Subject Authorization template has been designed to incorporate standard language for the statements required above. This template is available in IRBNet in Forms and Template. Inves

process. A full committee review will be required in those circumstances where a waiver has been requested by risk to the subject's privacy is considered to be greater than minimal. The IRB follows the Common Rule when reviewing the waiver request. Once the IRB has approved the waiver of authorization, the investigator must provide the covered entity maintaining the PHI with documentation from the IRB of approval. A waiver of authorization may be sought for three specific research uses of PHI to identify potential research subjects through:

- review of their PHI
- to contact potential subjects in order to determine their interest in research participation
- to receive or collect PHI during the conduct of research studies

Reviews Preparatory to Research

The Privacy Rule recognizes the necessity of accessing PHI, without patient authorization, in order to prepare a research protocol. This "preparatory to research" provision may be useful for examining
medic1d[(to6Tc 00 0 0.980.98 9)T(0.0143 Tc 0 Tw 118244 0 0 10.98.14.2445619498 Tm(in)Tj0.0002 Tc 0.4429 T
of

patient

hyt

Forms and Templates. This certification should be given to the holder of medical records for access to the information.

Research Involving the Use of Limited Data Sets

Regulations permit covered entities to use or disclosure PHI for research purposes without subject authorization if the use or disclosure only involves a "limited data set" and the covered entity enters into a data use agreement with the investigator. A "limited data set" is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual subjects:

- Names
- postal address information, other than town or city, state and zip code
- telephone numbers
- fax numbers
- email addresses
- social security numbers
- health plan beneficiary numbers
- account numbers
- certificate/license numbers
- vehicle identifiers and serial numbers
- device identifiers and serial numbers
- web universal resources locators (URLs)
- Internet protocol (IP) address numbers
- biometric identifiers, including finger and voice prints
- full face photographic images and any comparable images

A limited data set may, however include other indirect identifiers such as:

- City, State, 5-digit zip code
- Dates of birth, admission / treatment, discharge, death, etc.

A Limited Data Set is considered to be protected health information under the Privacy Rule. For this reason, the researcher must negotiate a Data Use Agreement for the project. The agreement must contain the following elements:

- The permitted uses and disclosures by the recipient
- The approved users and recipients of the data
- Agreement by the recipient not to re-identify the data or contact the individuals
- Assurances that the recipient will use appropriate safeguards to prevent use or disclosure of the limited data set other than as permitted by the data use agreement
- Agreement that the researcher will report to the covered entity any uses or disclosures of the limited data set which were not specifically allowed
- Agreement to require that any agents and subcontractors adhere to the same safeguards

Investigators may use or disclose a limited data set without subject authorization for research purposes only if an assurance is obtained in the form of a Limited Data Use Agreement available in IRBNet Forms and Templates.

De-identified data, Subject's Rights, and Recruitment

De-Identified Information

The de-identified health information under HIPAA is much more specific than the general de-identification standard applied under the federal laws relating to human research subjects. PHI can be released freely if it does not contain "individually identifiable information." PHI is not individually identified if the subject is not identified, directly or indirectly, and has no reasonable basis to believe that the information can be used to identify the subject. For example, a de-identified data set might include age, gender, marital status, ethnicity, diagnosis codes, and other medical data or an unidentified tissue sample. It may be used in research without subject authorization or a waiver of authorization. The Privacy Rule refers to such health information as "de- identified data." Research which involves the use of "de-identified data" is exempt from the HIPAA requirements. To be exempt from HIPAA, none of the 18 subject identifiers can be reviewed or recorded by the research team. In order to de-identify PHI, the investigator will comply with one of the two following procedures:

A. *Use of a Statistician to include:*

- Obtain services of a person with appropriate experience and knowledge applying generally acceptable statistical and scientific principles and methods for determining that the information is not individually identifiable;
- Who makes a determination that there is a very small risk that the information could be used by itself or in combination with other available information by the anticipated recipient(s) to identify the subject with the information; and
- Who documents the methods and results in making such determination.

B. *Removal of all identifiers*

- Removal of all18 identifiers listed above in the PHI section and have no actual knowledge that the information remaining could be used alone or in combination with other information to identify the patient who is the subject of the information.

Research subjects' rights under HIPAA

Right to an accounting:

When a research subject signs an authorization to disclose PHI, the covered entity is not required to account for the authorized disclosure. Nor is an accounting required when the disclosed PHI is contained in a limited data set or is released to the researcher as de-identified data. However, an accounting is required for research disclosures of identifiable information obtained under a waiver or altered authorization, reviews preparatory to research and research on decedents.

In addition to posting and providing a Notice of Privacy Practice, the covered entity must provide an accounting of all disclosures of an individual's PHI within the previous six years, upon request. It is anticipated that requests for an accounting of disclosure will come to the hospitals and the medical records department will respond in accordance with the policy on HIPAA: Accounting of Disclosures.

Right to revoke authorization:

A research subject has the right to revoke his or her authorization unless the researcher has already

Pre-screening Logs

Pre-screening logs which are used to document recruitment efforts in clinical trails often include PHI, such as initials, or dates of procedures. These logs should NOT be shared with a pharmaceutical sponsor without some form of privacy protection. In order to comply with the Privacy Rule, the data may be de-identified prior to sharing with the study sponsor. Alternately, if de-identified data is not feasible, the study sponsor can sign a Data Use Agreement and obtain the information in the form of a Limited Data Set.

Repositories and Databases

Research Repositories:

It may be necessary to create a repository that will support future research activities. The Privacy Rule specifies three ways in which PHI can be compiled for a research repository:

- individual, written authorization obtained from the subject
- waiver of the individual authorization requirement obtained from an IRB
- the PHI is obtained from a covered entity in a limited data set and accompanied by a data use agreement

If the repository is being created as new patients come to USA hospitals, the collection of data or

waived.

Research Databases:

If a researcher maintains a database containing PHI, then the investigator has an obligation to insure that the

Security

Computer Security for Research Records

HIPAA requires that privacy of PHI be maintained by limiting its use and maintaining appropriate computer security. Basic and well-established security principles will support our compliance efforts. These include:

- practicing "role-based access" to ensure that permissions for research files are commensurate with the employee's role in the project
- establishing password protections on electronic files
- storing records on secure networks and servers
- assuring that release of computerized research records conforms to HIPAA rules about allowable disclosures

HIPAA Security Measures

HIPAA requires that we maintain the privacy of PHI by limiting its uses and disclosures and that reasonable steps be taken to ensure that PHI is secure. Typically, breeches in privacy can be traced to relaxed security, therefore some steps to secure data include:

¾ Access to paper files be limited by locking file cabinets or locking rooms with files

¾ Avoid sending PHI in email or as email attachments. Email attachments should be password protected and possibly may require encryption depending on the sensitivity of the data.

¾ Password protection on all computers maintaining PHI

¾ Databases containing PHI may need additional level of password protected in order to restrict access to the database itself

Conclusion

The right to privacy in research has long been recognized as foundational to ethical conduct. Individuals wish to be asked about the use of their medical records for research and we must protect their privacy and dignity when using their medical information. As a result, the Privacy Rule creates expanded rights for research subjects and significant legal obligations when protected health information is used for research purposes. USA policies and procedures address these requirements as outlined in this tutorial and the HIPAA Compliance Plan for Clinical Research available at: http://www.southalabama.edu/departments/research/compliance/humansubjects/hipaa.html

Questions?

If you have any questions regarding the content of this training material or it's applicability, please email Ms. Dusty Layton, Office of Research Compliance and Assurance at dlayton@southalabama.edu or call 460-6625.

Additional Resources

Additional information and resources regarding the HIPAA Privacy Rule are available at:

DHHS Office of Civil Rights HIPAA Website: https://www.hhs.gov/hipaa/

National Institutes of Health: HIPAA Privacy Rule- Information for Researchers
https://privacyruleandresearch.nih.gov/pr_02.asp

Resources referenced to create this training module include:

USA HIPAA Research Website (HIPAA Research Compliance Plan):
http://www.southalabama.edu/departments/research/compliance/humansubjects/hipaa.html

Office for Civil Rights HIPAA Guidance, December 2002

University of Kansas Medical Center

HIPAA Research Tutorial

Health Insurance Portability and Accountability Act

Please save this page as your certificate of completion,
attach this certificate into your IRBNet User Profile,
and submit to the IRB for review

By selecting the checkbox and entering my name below, you confirm that you have received educational materials regarding the Privacy Rules and its impact on University of South Alabama (USA) Research. You understand that the Privacy Rules govern the ma
Compliance Plan for Research.

from you Supervisor or the Office of Research Compliance regarding

to privacy compliance activities. You will also report to your Supervisor or the Office of Research Compliance any suspected violations of the USA HIPAA Privacy Compliance Plan

You acknowledge understanding of the above info
HIPAA
Privacy Compliance Plan for Research.

Name: _____ Date:_____

If applicable, please enter your advisor's name below:

Advisor's Name: _____