Health Insurance Portability and Accountability Act (HIPAA)
Standards for Privacy of Individually Identifiable Health Information – (Privacy Rule)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed by Congress as Public Law 104-191. The “insurance portability” side of the law restricts insurers from rejecting health insurance coverage for individuals with pre-existing conditions such as cancer or heart disease; the “accountability” side of the law addresses security and protects the privacy personal health information.

DHHS has implemented the accountability requirements under the “Standards for Privacy of Individually Identifiable Health Information”, now commonly called the “Privacy Rule”. This Rule establishes the conditions under which personal health information may be used or disclosed for marketing, accounting, treatment and research purposes. The regulations were first published on December 28, 2000, subsequently modified and re-released as a final rule on August 14, 2002, Federal Register Volume 67, Number 157 p. 53181 – 53272 which amends CFR 45 Part 160 and 164. The specific provisions for research use and disclosure are covered under Part 164.501, 164.508(f) and 164.512(i).

Summary

The Privacy Rule sets standards for the security and privacy of personal health information and gives individuals more control over how this information, which could lead to identification, is used or released.

The application of the Privacy Rule is broader and separate from any other informed consent signed by a subject in an ongoing research project because it governs access to all individual medical records not just those typically collected by physicians or found at doctors’ offices, hospitals, and medical clinics. This same rule requires an authorization (either individual or waiver approved by an institutional review board) when personal health information that could be used to identify a specific individual is collected for research purposes or released to any outside party.

Basic health data included in employment or academic records, such as vaccination records, and anonymous personal health information are exempt from provisions of the rule. Likewise the publication of aggregate data is not restricted by these regulations, as the rule is not intended to limit a researchers’ ability to publish unless disclosure of identifying health information is involved.

The Privacy Rule applies equally to research that is publicly and privately funded and is supplemental to and does not supercede other federal regulations or state law which may be more restrictive. For example, federally funded research involving human subjects is also governed by the “Common Rule” and/or the Food and Drug Administration human subject protection regulations at 21 CFR Part 50.
What is the difference between the Privacy Rule and other federal regulations? The Common Rule and the FDA regulations require that research subjects be fully informed of the risks and benefits involved in their participation and that their identities remain anonymous. Whereas, the Privacy Rule addresses the confidentiality of records and requires separate permission whenever research involves the use or release of personal health information which could be used to identify an individual.

It is important to note that access to research data needed to conduct research may be denied, delayed or otherwise affected by a provider of data (medical doctors, hospitals and clinics) separately responsible for complying with the privacy rules.

ASU is considered a hybrid entity – one whose business activities include both covered and non-covered functions. The covered activities include:
- Campus Health Services
- Speech and Hearing Clinics
- College of Nursing and Healthcare Innovation’s Health Clinics
- Center for Health Information and Research
- University Technology Office

Compliance with information protection and use requirements is the responsibility of the principal investigator (PI) and his/her team. Each PI should periodically review their procedures to ensure that all protections are in place. It is the PI’s responsibility to assign a Privacy Officer and a Security Officer and to discuss their particular protection requirements with their School/College and also with the University’s Privacy and Security Officers.

**Procedures**

This Compliance Brief clarifies the implementation of the HIPAA Privacy rule by Arizona State University (ASU). The Institutional Review Board (IRB) will assume the responsibilities of the Privacy Board (PB). All activities constituting human subjects research must be review by an IRB prior to initiation of the research in accordance with regulations of the Department of Health and Human Services (45 CFR 46).

In addition, the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), effective April 14, 2003, governs the use of data involving protected health information by investigators who are part of a covered entity as defined by HIPAA. The Privacy Rule also governs disclosures of data to individuals, whether affiliated with the covered entity or not, who propose to use such data for research purposes. ASU is, as stated above, a hybrid entity per HIPAA criteria.

ASU’s HIPAA policies require that human subjects research subject to HIPAA that involves the use of protected health information must meet one of the following criteria:
- a HIPAA Authorization will be signed by the study participant;
- a HIPAA Waiver of authorization will be obtained from the IRB;
- the activity qualifies as preparatory for research;
• the researcher uses information solely on decedents;
• the information is completely de-identified and no longer governed by HIPAA;
• the information is compiled into a “limited data set” and a data use agreement is executed.

Review of Exempt Research

Proposals that qualify as exempt research under 45 CFR 46 must be submitted to the IRB, per ASU policy, and conducted in compliance with the Privacy Rule to the extent that the research involves the creation or receipt of protected health information about patients or research subjects, or the use or disclosure of protected health information maintained by or on behalf of ASU. Research protocols that meet these criteria will have to be submitted to the IRB with all required documentation/form(s) prior to initiating the protocol.

An investigator who seeks to conduct exempt research involving protected health information must:

1. Obtain from each research participant (or the participant’s legal representative) a signed, written authorization to use and disclose the participant’s protected health information for the research purpose;
   
   or

2. Obtain documentation of a waiver of authorization to use and disclose participants’ protected health information for the research purpose from the IRB; or

3. Enter into a data use agreement which permits the investigator to conduct research using a Limited Data Set of protected health information.

Thus, despite the fact that such research is not subject to the requirements of 45 CFR 46, the ASU IRB reviews all proposals for exempt research, and will also review the research for the purpose of granting a waiver of authorization, approving a research authorization form, or endorsing the use of a data use agreement under the Privacy Rule.

ASU Policy requires that all investigators involved in human subjects research complete the appropriate online training module. For more information see: http://researchintegrity.asu.edu/training/.

The regulations permit the use, release or disclosure of individually identifiable personal health information when specific written permission is given by the patient or, if individual authorization is impractical or if the risk of disclosure is low, when an institutional review board approves a waiver of individual authorization.

If the patient is also participating in the research project as a human subject, then the Principal Investigator is required to fulfill both the requirements for informed consent, including anonymity, and a separate authorization for the use or release of personal health information.

The regulation allows the use of a single form to gather the necessary approvals, so long as the approvals are separate and distinct.
Separate guidance will be distributed regarding the responsibilities of the institutional board responsible for implementing the rules for institutional review and approval of waivers of individual authorization.

Handling of Sensitive Information (e.g., HIPAA, IRB, Sensitive, Classified Information, etc.):
1. No HIPAA protected data may be stored on a personal computer.
2. Use of personal computers to stored university data is not allowed.
3. Data must be segregated from master lists; these must be stored on separate secure computers/servers.
4. Data should be encrypted whenever possible; password protection is not adequate. Appropriate firewalls must be in place.
5. Encryption is required when sensitive files are sent via email.
6. Passwords must be individually assigned and not shared. They should be routinely changed.
7. Users’ accounts must be removed if they no longer have a reason to access the information.
8. Computers must be properly maintained; software patches applied promptly.
9. Rooms/suites need to be locked and access limited.

Definitions

**Anonymity** means the quality or state of being unknown.

**The Common Rule** guides the majority of federal agencies as federal policy for the protection of human subjects. The rule contained in 45 CFR 46, was adopted in 1991 following a decade in which different agencies had different requirements; Subpart A relates to human subject research is known as the Common Rule. Seventeen federal agencies adopted the Common Rule for their individual needs. Each agency’s regulations are printed in the appropriate Code of Federal Regulations (CFR) and the text of the regulations relating to Subpart A are identical.

**Confidential** means information that is shared for a specific purpose with the expectation of confidence (as with an attorney, physician or spouse).

**Exempt Research** is research that involves human subjects but is not subject to the requirements of 45 CFR 46 or 21 CFR 56.104. Review by the IRB of projects described in 45 CFR 46.101(b) is required per institutional policy.

**Individual** means the person who is the subject of protected health information.

**Individually Identifiable Health Information** means information collected both orally or in writing that relates to a person’s past, present or future physical or mental health that could be used to identify an individual. Examples of information that could lead directly to identification are name, address (physical or electronic), telephone number, social security or other specific identity number such as an employee identification or drivers license number. Information that would not lead directly to individual identification might include hair color, eye color, height, weight, gender

**Informed Consent** the most comprehensive definition of informed consent is found in the first principle of the Nuremberg Code. The code states that voluntary consent of the human subject is absolutely essential. Voluntary consent means that the person involved should have legal capacity to give consent; be so situated as to be able to exercise free power of choice, without the intervention of any element of force, fraud, deceit, duress, over-reaching, or other form of constraint
or coercion; and have sufficient knowledge and comprehension of the subject matter and the elements involved as to enable him or her to make an informed and enlightened decision.

**Nuremberg Code** is the first set of formal guidelines which provided protection for human subjects participating in research. The guidelines were formalized in 1946 as a result of biomedical research performed during WWII. This code consists of a set of ten rules, some general, some specific, intended to guide researchers in the ethical conduct of biomedical research.

**Privacy Board** overseeing body for research practices with responsibilities much like an IRB. Privacy board responsibilities must be separately identified but may be delegated to an already standing IRB. This group serves to approve and oversee activities related to issues involving protecting private health information of human subject participants.

**Privacy Rule** discussed here is the comprehensive federal policy for the protection of personal health information used or disclosed for marketing, accounting, treatment and research purposes.

**Protected Health Information** means individually identifiable health information transmitted or maintained in any form or medium.

**Research** is a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of research repositories and databases for research purposes.

**Review Board (IRB)** means an Institutional Board established in accord with and for the purposes expressed in regulations that provide for the protection of human subjects.

**Waiver** means a document that evidences an intentional relinquishment of a right, claim or privilege.

**Related Resources:**

