

AUBURN UNIVERSITY 2008 HIPAA SURVEY

What is the HIPAA Privacy Rule?

The Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”) established, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The Privacy Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA. The Privacy Rule standards address the use and disclosure of individuals’ health information—called “protected health information” by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals’ privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights (“OCR”) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

A major goal of the Privacy Rule is to ensure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

Auburn University’s HIPAA Status as a Hybrid Entity

The entities covered by the Privacy Rule (“covered entities”) are those health care providers, health care clearinghouses and health plans that conduct specified transactions electronically. Auburn University is not primarily engaged in the activities that define a covered entity but may have some units that perform functions that fit the “covered entity” definition.

Under the Privacy Rule, any entity that meets the definition of a covered entity, regardless of size or complexity, generally will be subject to the Rule in its entirety. However, the Privacy Rule provides a means by which many covered entities may avoid global application of the Rule, through the **hybrid entity** designation provisions. This designation will establish which parts of the entity must comply with HIPAA. ***The hybrid entity is required to document identification of those of its units that perform covered functions (“covered units”).*** At this time, Auburn University is designated as a hybrid entity.

Any single legal entity may elect to be a hybrid entity if it performs both covered and noncovered functions as part of its business operations. A covered function is any function the performance of which makes the performer a health plan, a health care provider, or a health care clearinghouse. *To become a hybrid entity, the covered entity must designate the health care components within its organization. Health care components must include any component that would meet the definition of covered entity if that component were a separate legal entity.* A health care component may also include any component that conducts covered functions (i.e., noncovered health care provider) or performs activities that would make the component a business associate of the entity if it were legally separate. HIPAA governs only the protected health information created, received, or maintained by, or on behalf of, these components.

Any component part of a larger organization that answers affirmative to all of the following questions may be subject to HIPAA and its requirements:

1. Does the component (in whole or in part) perform any of the following covered functions...?
 - provide [for] or pay the cost of medical care;
 - provide [direct] medical or health services (or furnish, bill, or receive payment for health care in the normal course of business); or receive, process, or facilitate the processing of health information received from another entity into standard or nonstandard formats.

2. Does the component electronically receive or transmit individually identifiable health information pertaining to...?
 - health plan enrollment (or disenrollment);
 - health plan eligibility determinations;
 - health plan premium payments;
 - referral certification, authorization;
 - claim submissions (encounter info);
 - health plan benefit coordination;
 - claim status inquiries;
 - payment and remittance advices;
 - first report of injury; and/or
 - health claim attachments.

Key Definitions

The purpose of this survey is to help the University analyze whether HIPAA Regulations will apply to your particular school, department or unit. When responding to the survey questions, please use the following definitions.

Business Associate = an entity (including perhaps another AU department) that performs, or assists in the performance of, a function or activity that involves the "use" or "disclosure" of individually identifiable health information on behalf of the University.

Disclosure = the release, transfer, granting access to, or divulging in any manner Individually Identifiable Health Information outside your department/unit at the University or outside AU.

Covered entity = A health plan, health care clearinghouse or health care provider who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Generally, these transactions concern billing and payment for services or insurance coverage.

De-Identified Information = Health information that does not identify an individual, and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

Health Care = Care, services or supplies related to the health of an individual, and includes but is not limited to sale or dispensing of a drug, device, equipment or other item per RX or preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body.

Health Care Clearinghouses = Health care clearinghouses are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information. Health care clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.

Health Care Provider = A provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

Health Information = Any information, whether oral or recorded in any form, that is created or received by the covered entity that relates to an individual's past, present, or future physical or mental health, or to the payment for such health care.

Health Plan = Individual and group plans that provide or pay the cost of medical care. Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity.

Individually Identifiable Health Information = information that is created or received by the University that relates to

- the past, present, or future physical or mental health/condition of an individual; or
- the provision of health to an individual; or
- the past, present or future payment for the provision of health care to an individual

AND

- that identifies the individual; or
- with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information (PHI) = Individually Identifiable Health Information that is transmitted by electronic media, maintained in any electronic format or transmitted or maintained in any other form or medium. The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

The Privacy Rule defines PHI to include information that:

- is created or received by a “covered entity,” including a health care provider, and
- relates to the past, present, or future physical or mental health, or condition of an individual, or
- relates to payment for an individual’s health care, or
- relates to the provision of health care in the past, present, or future, and
- identifies an individual or could be used for identifying an individual.

In order to be de-identified, health information must be stripped of all of the following elements:

- Names;
- Social Security numbers;
- Telephone numbers;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly related to an 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;
- Fax numbers;
- Electronic mail addresses;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the research data)

Under HIPAA, information is considered de-identified if all of the above have been removed, and there is no reasonable basis to believe that the remaining information could be used to identify a person.

Note: Educational records protected by the Family Education Right and Privacy Act (FERPA) are exempt from the definition of PHI.

Use = the sharing, employment, application, utilization, examination, or analysis of Individually Identifiable Health Information within your department/unit at the University.

Helpful HIPAA Links

Detailed Overview of the HIPAA Privacy Rule

<http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf>

Summary of the HIPAA Privacy Rule

<http://www.hhs.gov/ocr/hipaa/privacy.html>

Covered Entity Charts

<http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf>

Fact Sheet: Privacy and Your Health Information

http://www.hhs.gov/ocr/hipaa/consumer_summary.pdf