

THE IMPACT OF THE HIPAA PRIVACY RULE ON RESEARCH AT UA

This document is currently a DRAFT IN PROGRESS. Send comments, suggestions, criticisms, areas for improvement, etc. to Jan Chaisson, UA HIPAA Privacy Officer. We need and value your input into this very important training tool!

I. AN OVERVIEW OF HIPAA COMPLIANCE

A. What is HIPAA and How Does It Apply To Research at UA?

1. Three Sets of HIPAA Regulations to Comply With

The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996 to:

- insure the portability of insurance coverage as employees moved from job to job;
- increase accountability and decrease fraud and abuse in health care; and
- improve the efficiency of the health care payment process, while at the same time protecting a patient's privacy (known as the Administrative Simplification provisions).

This latter goal was not achieved by Congress. By statute, the job of administratively simplifying the health care system was shifted to the Department of Health and Human Services (HHS). HHS has since 1996 promulgated different sets of regulations that require *covered entities*

- a) to engage in more standardized electronic sharing of health information (Standard Electronic Transactions/Code Sets Regs),
- b) to ensure the privacy of a patient's "protected health information" (hereinafter "PHI") (Privacy Rule), and
- c) to ensure the security of PHI (Security Regulations).

Pursuant to HHS's three sets of regulations, by October of 2003, all covered health care providers and health plans will be required to use standardized electronic transactions and code sets for data that will facilitate a more cost efficient transfer of PHI. By April 14, 2003, all *covered entities* will be required to comply with Privacy Regulations. *Covered entities* must also comply with the Security Regulations; however, no compliance deadline has been set because HHS has not yet issued its final HIPAA Security Regulations. The purpose of this document is limited to describing the impact the Privacy Rule will have on research at The University. Additional requirements will be imposed on "*covered entities*" and researchers once the Security Regulations are finalized. A "*covered entity*" will hereinafter be referred to as CE.

2. What is a Covered Entity, Hybrid Entity, & Health Care Component at UA?

The Privacy Regulations do not apply to all health information obtained by any university researcher. Rather, the rules discussed below apply only to PHI used or disclosed by a CE. Generally speaking, a CE may freely use or disclose PHI for treatment, payment, or health care operations (TPO). The use/disclosure of a CE's PHI for research purposes is not considered TPO. A CE may also disclose PHI pursuant to the HIPAA laws and regulations. If the use/disclosure of PHI is not for TPO or otherwise authorized by law, then the CE cannot use/disclose the PHI unless the patient signs a valid HIPAA authorization. Requiring that every researcher in every situation obtain an authorization to use an individual's PHI could significantly damage research production in the United States. To avoid that result, a CE may still disclose PHI to a researcher if the researcher obtains a "waiver of authorization" from an IRB.

Because the Privacy Rule only applies to PHI flowing from a CE, it is critical to first understand which organizations qualify as a CE. A CE is defined in the Privacy Rule as

- a health care provider that conducts certain transactions in electronic form,
- a health care clearinghouse,
- a health plan, or
- a business associate (person or organization performing a function on behalf of the CE for which access to PHI is needed).

Because the University of Alabama has at least one department that provides health care services and electronically transmits a "standard transaction,"¹ it is considered a CE. Since the primary function of UA is not to provide health care, UA is permitted to designate itself as a "hybrid entity," which allows it to apply the Privacy Rule only to those parts of UA that, if standing alone, would be a CE. A hybrid entity must designate its "health care components" (hereinafter "HCC"), which should include departments which provide support for the HCC (like Legal Office, Accounting Office, etc.).

¹ Covered standard transactions for health care providers are, for the most part, associated with third party billing. Some (but not all) covered standard transactions include:

- a request to obtain payment, and necessary accompanying information, from a health care provider to a health plan for health care
- if there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care
- an inquiry (or a response) from a health care provider to a health plan (or between health plans) to obtain any of the following information about a benefit plan for an enrollee
 - eligibility to receive health care under the health plan
 - coverage of health care under the health plan
 - benefits associated with the benefit plan
- a request (or response) for the review of health care to obtain an authorization for the health care
- a request (or response) to obtain authorization for referring an individual to another health care provider

Only the HCCs of a hybrid entity must comply with the Privacy Rule, and at UA the following departments will be designated HCCs subject to the Privacy Regulations:²

- Capstone Medical Center
- Brewer-Porch Children’s Center
- Russell Student Health Center
- College of Nursing’s Capstone Rural Health Center in Parrish
- Speech and Hearing Clinic
- The Office of Counsel, the Office of Financial Accounting, and/or the Auditors may also be deemed administrative support units of these HCCs.

The University’s self-insured health plan also has compliance responsibilities unique to health plans.

3. Sharing of PHI for Research in a Hybrid Entity

Generally speaking, any employee of a HCC at UA must not disclose PHI in its possession to UA employees working in other HCCs or other departments at UA, unless

- the information is shared for Treatment, Payment, or Health Care Operations (TPO), or
- the patient has signed a *valid* HIPAA authorization.

These restrictions impact the use of PHI for research purposes. For example, if the Capstone Medical Center uses/discloses any PHI to any UA faculty, graduate or undergraduate student conducting research, then it must conform to the new Privacy Rule research requirements discussed below or face serious penalties. If, on the other hand, the School of Social Work, which is not currently designated as a HCC, collects PHI directly from patients/clients for research purposes, the provisions of the Privacy Rule pertaining to use/disclosure for PHI do not currently apply to that research project. The IRB, however, will still be interested in obtaining from the researcher written assurances of how he/she plans to protect the privacy of the research subject’s health information.

If a university does not designate itself as a hybrid entity, but has at least one department that makes it a CE under HIPAA, then *all* research involving the use/disclosure of PHI obtained at that CE must comply with the Privacy Rule. It is clearly more advantageous for a university to designate itself as a hybrid entity to eliminate as much activity as possible from the HIPAA criminal and civil penalty scheme.

² Other units on campus may provide health care services as defined in the Privacy Rule, but do not engage in the electronic transmission of a covered standard transaction. Also, other units on campus may maintain individually identifiable health information in a student’s education record covered under FERPA’s Policy on Confidentiality of Student Records, or in employment records. Those units do not have to be designated as health care components, and thus will not be subject to Privacy Rule requirements and penalties. Although exempt from HIPAA, good risk management and prudence suggests that steps be taken to heighten awareness of confidentiality expectations in those departments to avoid state tort breach of privacy claims, which will likely increase due to patients’ heightened awareness of their privacy rights.

In sum, the HIPAA Privacy Rule does NOT apply to:

- research that uses or discloses information that is not defined to be PHI (health information protected by FERPA or in an employment record, or non-health information)
- research that uses PHI collected in a program that is not part of the hybrid CE's HCC
- research that uses PHI collected from a non-covered entity.

If the researcher obtains information from any entity other than the research subject itself, then the researcher should understand whether the provider of the information is an CE or a HCC within a hybrid entity. In both those instances, the HIPAA Privacy Rules regarding research activities would apply.

While research approved by the IRB and initiated before April 14, 2003 is excluded from the new research requirements (see Transition Provisions at end of this document), researchers at The University of Alabama must be trained on the Privacy Rule requirements related to research and the IRB must ensure compliance by April 14, 2003 or face serious penalties.

B. HIPAA Penalties

Serious criminal penalties are associated with failure to comply with HIPAA requirements. The employees, students, interns, and residents of a CE or of a HCC of a hybrid CE

- who wrongfully use/disclose PHI are personally at risk for fines up to \$50,000 and/or 1 year in prison;
- who obtain PHI under false pretenses are subject to fines up to \$100,000 and up to five years in prison; and
- who use or disclose PHI for commercial gain, including those who fail to comply to HIPAA requirements while conducting research that is considered a commercial activity (paid for by a sponsor, or development of a device or discovery that can be sold), will be subject to penalties up to \$250,000 and up to ten years in prison.

In addition, civil penalties can be imposed on the University or one of its employees for violations of HIPAA or its regulations. Civil penalties are limited to not more than \$100 for each violation, with a total civil penalty not to exceed \$25,000 in any given year.

Finally, civil monetary damages may be available to patients who successfully pursue state tort claims, such as breach of privacy claims and those common in human subject litigation.

C. Definitions Pertinent to Covered Research Activities

1. **What is protected health information?** Protected Health Information (PHI) is all individually identifiable health information (oral or recorded in any medium), including demographic information, that relates to the past, present, or future physical or mental health or condition of any individual; the provision of health care to any individual; or the past, present or future payment for the provision of health care to any individual. PHI does not, however, include individually identifiable health information in education records, which are protected by the Family Educational Rights and Privacy Act and the University's Policy on Confidentiality of Student Records (accessible on the web at <http://registrar.ua.edu/policies/ferpa.html>). Nor does PHI include health information collected and maintained in employment records for various employment purposes.

Researchers who compile and analyze data about the physical or mental health of any population and who obtain that information from a CE or a HCC of a hybrid CE are immediately engaged in handling PHI. A CE releasing to a researcher will have to ensure that it complies with HIPAA Privacy Rules, or risk serious penalties. All researchers, however, have in the past been subject to IRB-approved protocols for protecting the confidentiality of a research subject's health-related information.

2. **What is research?** Research is "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." (45 CFR §164.501). This definition of "research" in the Privacy Rule is consistent with what is considered "research" under the Common Rule (and thus includes the development of research repositories and databases for future research)

Research activities dealing with PHI must meet the standards of **both** the Common Rule and HIPAA. Compliance with HIPAA is in addition to (*not instead of*) the Common Rule requirements. The Privacy Rule strengthens existing human subject privacy protections for research and creates equal standards for privacy protection for research governed by the Common Rule and FDA and research that is not covered.

3. **What Does the Common Rule Require?** Under the Common Rule applicable to federally regulated human subjects research, researchers must either have the informed consent of anyone participating in a research study, or a waiver from the Institutional Research Board (IRB). As part of the IRB's process to approve research and as a requirement for informed consent, researchers currently must describe the extent to which confidentiality of records will be maintained. In approving the research, an IRB is currently required to consider whether there are adequate provisions in the protocol to protect privacy of subjects and to maintain the confidentiality of data. 21 CFR § 46.111 (a)(7). This requirement remains in place for all research, whether the PHI comes from a CE, HCC of a hybrid CE, or a non-CE.

II. The HIPAA Privacy Rule Requirements for Research When the Data Flows from a Covered Entity or Health Care Component of a Hybrid Entity

A. Authorization or a Waiver of Authorization from the IRB

Unless one of the exceptions mentioned in Section B below applies, researchers using PHI obtained from a CE or HCC of a hybrid CE must either

- receive a valid HIPAA *authorization* from the patient or subject in the study to use/disclose the PHI for research purposes, or
- obtain a *waiver of HIPAA authorization* from the researcher's or CE's IRB (or separate Privacy Board).

1. Requirements of a Valid Authorization

To be valid, a HIPAA authorization must contain the following core elements and statements (45 CFR § 164.508 (c)):

1. a specific description of the information to be used or disclosed by the researcher, which must be "research study specific;"
2. the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure of PHI and to whom a covered entity is authorized to make the use or disclosure;
3. a description of each purpose of the requested use or disclosure (which cannot encompass future unspecified research);
4. a statement of the individual's right to revoke the authorization in writing, a description of how to revoke, and the exceptions to the right of revocation;
5. an expiration date or event, or a statement that there is no expiration date;
6. a statement describing whether or not the University is making treatment, payment, enrollment, or eligibility for benefits contingent on the authorization;
7. a statement that information disclosed pursuant to the authorization may be subject to further disclosure by the researcher and may no longer be protected by the Privacy Rule, and
8. a signature of the individual and date.

The authorization cannot authorize the researcher to use the data for future unspecified purposes. It must be written in plain language and a signed copy must be provided to the individuals participating in the research.

An authorization **MUST** be obtained from every participant in a research study, unless the IRB has provided a waiver.

The HIPAA authorization may be combined with any other legal permission related to that research study, such as the Common Rule's requirement of an informed consent signature for the same research project.

If a subject's PHI is to be used in more than one study, then there must be a separate signature authorizing the use of the data for each study.

If an individual revokes his/her authorization, the researcher may continue to use and disclose the PHI that has already been obtained to the extent that it is necessary to preserve the integrity of the research study. The IRB does not have to approve the continued use of PHI.

2. Waiver Criteria Required by the IRB

Per the comments in the final Privacy Regulations, a researcher's ability to use PHI without a patient's authorization is a privilege that requires strong confidentiality protections. To ensure that protection, HHS ultimately adopted three criteria that an IRB must examine to decide if a patient's authorization can be waived. 45 CFR § 164.512 (i). To provide a waiver, the IRB must find that:

1. The use or disclosure of PHI involves no more than *minimal risk to privacy* based on, at least, the presence of the following elements:
 - (a) an adequate plan to protect the identifiers from improper use and disclosure;
 - (b) an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
 - (c) adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by this subpart;
2. The proposed research could not practicably be conducted without the waiver or alteration, and
3. The research could not practicably be conducted without access to and use of the PHI.

The comments from HHS in the August 14, 2002 Federal Register explain that these three criteria safeguard patient privacy, require attention to issues sometimes currently overlooked by IRBs, and are compatible with the Common Rule.

HHS indicated it intends to issue further guidance on how to interpret these three waiver criteria. Some questions suggested to be answered include:

- Can the IRB find the research cannot practicably be conducted w/o waiver if the research: a) would be too costly or would involve excessive time and effort leading to unacceptable study delay; b) result in less than full or less than acceptable levels of participation by the target group, leading to biasing or failure of the study?

B. Four Exceptions to Authorization or Waiver of Authorization by the IRB

There are four exceptions to the Privacy Rule's requirement of getting an authorization or waiver of authorization: research on records of decedents, reviews preparatory to research, use of de-identification of data, and limited data sets.

1. **Research on records of decedents**: If a research subject is deceased, PHI from a CE (or HCC of a hybrid entity) may be used or disclosed provided that the researcher represents that the use or disclosure is sought solely for research on PHI of decedents, and PHI for which use or disclosure is sought is necessary for research purposes. The CE may request that the researcher provide documentation of the death of the individual.

2. **Reviews preparatory to research**: A CE (or HCC of a hybrid CE) may use or disclose PHI for reviews preparatory to research if the researcher represents that

- use and disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research (e.g., recruitment);
- no PHI is to be removed from the CE (or health care component of CE) in the course of the review; and
- the PHI being sought is necessary for the research purpose.

If the researcher is also the subject's treating physician, then the Privacy Rule permits the physician to recruit his/her patient for research without the patient's authorization. That is because the physician is only releasing to the patient information he/she legitimately has access to.

Testimony before a subcommittee of HHS on October 29, 2002 asked for clarification on these issues regarding recruitment:

- Does the researcher employed by the CE have the right to obtain PHI about patients of other physicians employed by the CE to recruit the patients for research? (If so, CCHS may want to be designated as an administrative support unit of Capstone Medical Center, so that researchers/physicians employed by either CCHS or CMC (or both), can more easily recruit patients of each other).
- Is access to the CE's PHI for recruitment purposes an internal use or a disclosure to a third party when the researcher is a "dual employee" of the medical school faculty and the separate physician practice group?

3. **De-Identification**: The HIPAA Privacy Rule's use and disclosure provisions do not apply to information that has been de-identified [45 CFR §164.514 (a-c)]. De-identification can be done through two ways:

- a) If a statistician concludes "the risk is very small that the information could be used, alone or in combination with other reasonably available information, by

an anticipated recipient to identify an individual who is the subject of the information”; or

- b) Through the safe harbor’s removal of the following 18 identifiers:
1. Names;
 2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, and in most cases, the whole zip code;
 3. 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;
 4. Telephone Numbers;
 5. Fax Numbers;
 6. Electronic mail addresses;
 7. Social security numbers;
 8. Medical record numbers;
 9. Health plan beneficiary numbers;
 10. Account numbers;
 11. Certificate/license numbers;
 12. Vehicle identifiers and serial numbers, including license plate numbers;
 13. Device identifiers and serial numbers;
 14. Web Universal Resource Locators (URLs);
 15. Internet Protocol (IP) address numbers;
 16. Biometric identifiers, including finger and voice prints;
 17. Full face photographic images and any comparable images; and
 18. Any other unique identifying number, characteristic, or code, except as permitted in paragraph c described next.

A CE may create a code or other means of record identification to allow de-identified information to be re-identified, provided that the code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and the CE does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification. [45 CFR §164.514 (c) (1 & 2)].

The HCC of a hybrid CE may designate who can de-identify data, and can give that authority to a third party, if the third party is covered by a HIPAA Business Associate Agreement.

4. ***Limited Data Sets:*** Finally, no authorization or IRB waiver is necessary to use/disclose a limited data set, if the information is being used for the purpose of research, public health or health care operations. Limited data sets still remove 16 of the 18 identifiers cited for de-identification, but allow the researcher to keep dates related to the individual (such as dates of birth and death, dates of admission and discharge, and

dates of service) and five-digit zip code information or other geographic subdivision information (city, county), except for street address. [45 CFR §164.514 (e)(2)].

A limited data set must exclude the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

1. Names;
2. Postal address information, other than town or city, State and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URL);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.

The researcher can use this limited data set, subject to the minimum necessary requirement of the Privacy Rule, so long as there is a **Data Use Agreement**. A DUA must, per 45 CFR § 512(e)(4):

- establish the permitted uses and disclosures of information by the limited data set recipient,
- establish who is permitted to use or receive the limited data set,
- provide that the recipient will
 - a. not use/further disclose information other than as permitted by DUA or by law;
 - b. use appropriate safeguards to prevent use or disclosure of the information other than as provided by DUA;
 - c. report to the CE any use/disclosure of the information not provided for by its DUA of which it becomes aware;
 - d. ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient; and
 - e. not identify the information or contact the individuals.

A breach of a DUA by the researcher (who is not a CE) is not a violation of HIPAA, but rather is a breach of the agreement. The CE is ultimately responsible for HIPAA compliance and must take steps to cure the breach or end the violation. If steps to end the violation are unsuccessful, the CE must discontinue disclosure to the researcher and

report the problem to HHS. If the CE is the recipient of the limited data set, and the CE violates the DUA, it will be in non-compliance with the HIPAA requirements.

One unanswered question is whether in a hybrid entity situation, where the recipient is also an employee of UA, but not of the HCC that provided the limited data set, can the UA employee can enter into a DUA with a UA HCC? (UA cannot enter into business associate agreements with each other: administrative units must be designated part of HCC to permit other departments to gain access to PHI of the HCC to perform work for that HCC)

C. Requirement of an Accounting for Waivers of Authorizations by IRB

Under HIPAA, a patient has a right to an accounting of disclosures for the past 6 years that have been made of their PHI by a CE. No such accounting is needed, however, when

- the CE uses/discloses the PHI for TPO
- the patient/subject has signed a HIPAA authorization
- the CE only released a limited data set and the recipient signed a DUA
- the information was de-identified.

If, however, a research study is conducted with an IRB waiver of the HIPAA authorization, or if a researcher has accessed health information for purposes preparatory to research, then the researcher must provide an accounting to all individuals in the study when PHI is disclosed, if the participants request an accounting. HHS recognized that this could be one of the most difficult compliance aspects of the waiver of authorization requirement. Generally, patients entitled to an accounting can request data during the six years prior to the date of request of an accounting. For each disclosure, the covered entity or researcher must reveal the name of the entity or person who received the PHI and their address, and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

D. Simplified Protocol Listing Alternative for Research-Related Disclosures w/o Authorization

Because the volume of individually tracking such records for some research projects presented an administrative obstacle for research, HHS adopted in the final Privacy Rule an alternative to the normal accounting required for disclosures. If the research disclosure involves at least 50 records, covered entities may provide individuals with a list of all protocols for which the patient's PHI *may* have been use/disclosed for research pursuant to a waiver of authorization, as well as the researcher's name and contact information. For research protocols for which the individual's PHI may have been disclosed during the accounting period (last 6 years), the accounting must include the name of the study or protocol, a description of the purpose of the study and the type of PHI sought, and the timeframe of disclosures in response to the request. When asked by the person, the covered entity must provide assistance in contacting those researchers to whom it is likely that the individual's PHI was actually disclosed. Also HHS has

encouraged the covered entities to list under separate headings, or on separate lists, all protocols relating to particular health issues or conditions, so that individuals may more readily identify the specific studies for which their PHI is more likely to have been disclosed.

Finally, the rule exempts from the accounting requirements disclosures made prior to the compliance date for the Privacy Rule, or April 14, 2003.

E. Grandfathering of Existing Research Data.

Health care components at UA (or a CE) may use and disclose PHI for research purposes from data sets it created or received either before or after April 14, 2003, provided there is no agreed-to restriction and the CE has obtained prior to April 14, 2003 either:

1. an authorization or some express legal permission from the patient to use the PHI for research; or
2. the informed consent of the individual to participate in the research, or
3. a waiver by the IRB of informed consent for the research, provided that a CE must obtain the HIPAA authorization if, after April 14, 2003, informed consent is sought from an individual participating in the research.

45 CFR § 164.532 (c).

*Prepared by the Office of Continuous Quality Improvement
The University of Alabama*