HIPAA Handbook for Researchers at UAB

Prepared by the
UAB Institutional Review Board for Human Use,
UAB Health System Information Services,
and the
UAB HIPAA Coordinator's Office

Date of First Publication: March 29, 2004
Revised: December 21, 2010

HIPAA Handbook for Researchers at UAB

Background and Purpose

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed into law on August 21, 1996. The portions of the regulations that are important for our ***research*** purposes are those that deal with protecting the ***privacy*** and security of ***protected health information (PHI)***.

The Privacy Rule regulates the way certain ***covered entities*** handle ***individually identifiable health information*** known as PHI. The Office for Civil Rights (OCR) in the Department of Health and Human Services (DHHS) oversees HIPAA Privacy Rule compliance; therefore, one of the best sources of information on the HIPAA Privacy Rule is the DHHS/OCR web site at www.hhs.gov/ocr/hipaa.

Like the Privacy Rule, the Security Rule affects covered entities that create, store, use or disclose PHI. Unlike the Privacy Rule, the Security Rule affects only PHI in electronic format (ePHI), not oral or paper-based PHI. The Centers for Medicare and Medicaid Services (CMS) oversee compliance with the HIPAA Security Rule. The CMS HIPAA web site can be found at http://www.cms.hhs.gov/HIPAAGenInfo.

This overview is intended for UAB researchers and their staff members. It does not contain all of the information that will affect each person who works with clinic ***patients***, research ***participants***, or potential participants. Researchers or their staff members who do not find the guidance they need in this overview should consult the Contacts and Resources sections of this document. Although this overview focuses on UAB's compliance with the HIPAA regulations, it also contains information regarding research compliance measures required by other federal regulations, UAB policy, and UAB IRB procedures. UAB's policies and procedures are more stringent than is required by the HIPAA regulations.

Terms in ***italic, boldface*** are in the Glossary on page 13.

Applicability

The HIPAA regulations mandate the way covered entities handle PHI. Researchers should be aware of the HIPAA regulations because they establish the conditions under which covered entities can use or disclose PHI for research purposes.

Research Regulations

The HIPAA regulations do not replace or reproduce other federal research regulations (e.g., 45 CFR 46, 21 CFR 56). All existing regulations related to our research activities remain in force. In fact, unlike some other regulations, HIPAA applies whether or not the research is funded by the government.

It is important to note that HIPAA preempts all less stringent state laws regarding privacy of health information unless specific requirements are met. In general, these requirements involve state-mandated reporting related to health, safety, or welfare, as well as reporting that is necessary for a health plan to conduct auditing procedures. Instructions for requesting an exemption—to follow the state law instead of HIPAA—are given in Subpart B of the Privacy Rule (§160.201-205).

All uses of PHI for research require an IRB-approved Human Subjects Protocol.

A covered entity may use or disclose PHI for research if the researcher has IRB approval and one of the following five conditions applies. Each of these conditions is explained more fully under the heading of Documentation:

1. The activity is preparatory to research.
2. The research involves only decedent PHI.
3. The research uses a ***limited data set*** and ***data use agreement***.
4. The patients/participants have signed an ***authorization*** to use their PHI for the research.
5. The IRB has waived or altered the requirements for patient/participant authorization.

HIPAA Identifiers (§164.514(b)(2)(i))

HIPAA lists 18 identifiers or data elements that must be absent before ***health information*** can be shared without the patient's authorization. If all 18 are removed from the data, then the data are considered ***de-identified***, or ***anonymized***. Anonymized data are not considered PHI and not affected by HIPAA.

The following 18 identifiers must be removed for the information to be considered de-identified:

1. Names
2. Geographic subdivisions smaller than a state
3. Elements of dates (except year) related to an individual
4. Telephone numbers
5. Fax numbers
6. Email 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
13. Device identifiers and serial numbers
14. Biometric identifiers
15. Web universal resource locators (URLs)
16. Internet protocol address numbers
17. Full-face photographic images
18. Any other unique identifying number (does not include codes as long as the research staff cannot link the data to an individual)

Statistical Determination

Covered entities can also use statistical methods to establish de-identification. The covered entity may obtain certification by "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" (§164.514(a)(1)) that there is minimal risk that the information could be used by the recipient to identify the individual who is the subject of the information.

Re-identifying Codes (§164.514(c))

The regulations take into account that workers in a health care organization may need to know the origin of PHI in a de-identified data set. Therefore, a health care organization may assign a code or other means of record identification to allow de-identified information to be re-identified by the health care organization. Two conditions apply to this code:

1. The ***re-identifying code*** must not be derived from or related to information about the individual and must not be otherwise capable of being translated so as to identify the individual; and
2. The re-identifying code must not be used or disclosed for any purpose other than re-identification, and the health care organization must not disclose the code or how it works.

Minimum Necessary Standard (§164.502(b))

When disclosing patient information, everyone who works at a health care facility must make a reasonable effort to use or disclose only the minimum information necessary to meet the intended purpose. This means that a covered entity must limit the PHI it releases to a researcher to "the information reasonably necessary to accomplish the purpose" (§164.514(d)(4)(i)). A covered entity will rely

on a researcher's request and the documentation from the IRB to define the minimum PHI necessary to accomplish research goals.

If a research participant signs a proper, IRB-approved authorization, then the minimum necessary standard is considered met. However, without such an authorization in place, the minimum necessary standard applies to the research activity.

A signed authorization supersedes the minimum necessary standard.

Clinical Confidentiality

Patient Rights

The HIPAA Privacy Rule guarantees patients certain rights regarding the ***use*** and ***disclosure*** of their PHI. Many of these rights relate to patients' privacy, ***confidentiality***, and access to medical records during treatment within a covered entity. However, if the PHI is released to a researcher, then that researcher becomes responsible for ensuring that those patients' rights are fulfilled regarding the use of PHI for research purposes. As described below, these guarantees of rights may require documentation on the part of the covered entity, the researcher, or both.

UAB Health System Accounting of Disclosures Administrative Standard: https://scr.hs.uab.edu

Access to Protected Health Information

The Privacy Rule grants individuals the right to access their medical records and other types of health information contained within a ***designated record set***. Research records maintained by a covered entity may be part of this designated record set.

In most cases, patients or research subjects are allowed access to their designated record set . One exception is during a clinical trial when the individual's right of access can be suspended while the research is in progress if, in consenting to participate in research that may involve treatment, the individual agreed to the temporary denial of access to these data. Individuals must be informed that the right to access their designated record set will be restored at the conclusion of the clinical trial.

Accounting of Disclosures for Research (§164.528)

A patient or a patient's legal representative has the right to receive an accounting of certain disclosures of PHI made by the University of Alabama at Birmingham (UAB) or the UAB Health System (UABHS) in the six (6) years prior to the date of the request, but not prior to April 14, 2003.

Covered entities are **not** required to track or provide an accounting for the following disclosures:

1. To carry out treatment, payment or health care operations (TPO).
2. To individuals about themselves.
3. For facility directory purposes.
4. To persons involved in the care of the patient.
5. For national security or intelligence purposes.
6. To correctional institutions or other law enforcement officials.
7. As part of de-identified data or a limited data set.
8. For disclosures made prior to April 14, 2003.
9. Pursuant to a valid authorization.
10. For incidental disclosures.
11. For other such reasons as allowed under HIPAA.

To account for research disclosures that were made without patient authorization, UAB/UABHS covered entities will rely on the alternative method of accounting by furnishing a list of protocols maintained by the UAB Institutional Review Board (IRB) that involve PHI and that fall in the following categories:

1. Waiver of authorization,
2. Activity preparatory to research, or
3. Decedent reviews.

Honoring a patient's request for an accounting of disclosures is to be managed by the covered entity's Entity Privacy Coordinator in conjunction with the Health Information Management Department and the UAB/UABHS Privacy Officer.

Basic Privacy and Security Practices

Many of the privacy and security practices used to protect patients' health information are things we do as professional and as common sense business practices. So, what things can be done to protect PHI and ePHI?

Privacy

- Don't discuss patients or participants in a public place (like a hallway or elevator) in such a way that someone overhearing you could identify the person.
- Don't leave medical or research records—whether printed or on a computer screen—unattended.
- Don't leave labeled tissue samples unattended.

Physical Security

- Store PHI in locked areas, desks, and cabinets.
- Control access to research areas.
- Obtain lock-down mechanisms for devices and equipment in easily accessed areas.
- Challenge persons without badges in restricted areas.
- Verify requests of maintenance, IT, or delivery personnel.

Internet and Email Use Security

- Do NOT email ePHI unless between GroupWise and Central Exchange email addresses. Confirm Central Exchange addresses with AskIT.
- If ePHI must be transmitted via email outside the GroupWise/Central Exchange systems, then the transmission must be encrypted. Ask your IT representative to assist you with encryption.
- Do NOT store ePHI on any website.

Desktop/Workstation Security

- Arrange computer screen so that it is not visible by unauthorized persons.
- Log off before leaving the workstation.
- Configure the workstation to automatically log off and require user to login if no activity for more than 15 minutes.
- Set a screensaver with password protection to engage after 5-10 minutes of inactivity.
- Manage your research data. Store documents and databases with ePHI securely on a network file server. Do NOT store ePHI on the workstation (C: drive).
- Do not allow coworkers to use your computer without first logging off.
- If you have permission to work from home or a remote location, contact your IT/IS department to securely configure the workstation.

Account Management

- Do not share your user account, password, token, or other system access. You are responsible for all actions associated with your user ID and password.
- Use strong passwords that are at least 6 to 8 characters long. Include upper- and lowercase letters, numbers, and special characters (#, %, ?, $).
- Do not use pet names, birthdates, or words found in the dictionary.
- If you must write down your password, keep it locked up or in your wallet protected like a credit card.
- Do not enable your browser to remember your password.
- Only access PHI/ePHI for business-related purposes.
- Do not use your system access to look up medical information on yourself, family, friends, or coworkers.
- Notify IT support immediately if you believe your system access has been compromised.

Portable Device Security

- Portable devices include hand-held, notebook, and laptop computers; personal digital assistants; cell phones; and pocket or portable memory devices such as thumb and jump drives.
- Do not use a portable device for storing ePHI.
- Use encryption when transporting ePHI on any mobile computing device. Be sure to backup encryption keys.
- Use password protection.
- Delete ePHI when it is no longer needed.
- Keep your application software up-to-date.
- Back-up critical software and data on a secured network.
- Follow all of the recommendations for workstation security.
- Use only VPN for remote wired and wireless connectivity.
- Check with IT representatives for other security safeguards.

Documentation

As do many federal regulations, HIPAA adds to the documentation required to conduct research. New documentation involves four categories:

- authorizations for use and disclosure of a patient's PHI,
- waivers and alterations of such authorization as granted by the IRB,
- limited data sets and data use agreements, and
- accounting of disclosures.

Authorizations (§164.508)

An authorization document describes how participants' PHI will be used and disclosed in relation to a specific research protocol. Authorizations must include

1. A description of the PHI to be used or disclosed, identifying the information in a specific and meaningful manner;
2. The people/organization(s) who may use the PHI, such as the Principal Investigator;
3. The people/organization(s) who will receive the information, such as the sponsor;
4. A statement that the parties receiving the disclosed information may not be bound by HIPAA privacy regulations and may re-disclose the information;
5. The purpose of the disclosure, usually as described in the study purpose and procedures;
6. An event when the authorization will expire—such as "End of study," "15 years after end of study," or even "never";
7. The participant's right to refuse authorization and whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on authorization;

8. The participant's right to revoke authorization in writing; however, PHI *collected before* the authorization was revoked may still be used to maintain scientific integrity of the study, such as to explain a participant's withdrawal or to report adverse events; and
9. Spaces for the patient's signature and the date of the signature.

Investigators should maintain all signed authorizations for six (6) years after the study is completed or for six (6) years after the authorization was signed, whichever is later. Accounting of disclosures is not required when an authorization is completed and signed by the patient or the patient's legal representative.

See a sample Authorization in this handbook or at www.uab.edu/irb/forms.

Consent Form

When researchers obtain a signature for informed consent from participants whose PHI will be used in a specific research protocol, the authorization should be the last page of the consent form for that protocol. The consent form is reviewed by the IRB as part of the Human Subjects Protocol review.

Waiver or Alteration of Authorization (§164.512(i))

With proper documentation from the researcher—and only for a single, specific protocol—the Institutional Review Board for Human Use (IRB) can review requests to waive part or all of the requirements for patient authorizations. The following three criteria must be satisfied for the IRB to approve a waiver of authorization under the HIPAA Privacy Rule:

1. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, 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 an 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 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 application for a waiver of patient authorization is available at http://www.uab.edu/irb/forms. An authorization can be combined with an informed consent document or other permission to participate in research; however, it must be approved by UAB Office of Counsel and contain specific core elements and required statements.

Reviews Preparatory to Research

Researchers are allowed to review a covered entity's PHI as part of their preparations for research, such as identifying potential participants. Three conditions apply to such waivers:

1. The researcher's use or disclosure is proposed solely to review PHI to prepare a research protocol or for similar purposes preparatory to research;
2. The researcher will not remove any PHI from the covered entity; and
3. The PHI that the researcher wants to use is necessary for the research purposes.

Investigators must describe the preparatory activity in the protocol itself and make the representations listed above.

Research on Decedent Information

If approved by the IRB, researchers are allowed to review a covered entity's PHI on decedents. Three conditions apply to such waivers:

1. The researcher proposes to use PHI of decedents only;
2. On request of the covered entity, the researcher will provide documentation that the persons are dead; and
3. The PHI is necessary for the stated research purposes.

Often, protocols that propose research on decedent PHI will qualify for Exemption Review from the IRB provided that (a) no personal identifying information will be collected in the review and (b) no contact with living relatives of the decedents is planned. Only the IRB can determine Exempt status. In any event, the investigator must make the representations listed above.

Limited Data Sets and Data Use Agreements (§164.514)

Limited data sets contain collected PHI that excludes certain direct identifiers. So long as a ***data use agreement*** is in place, limited data sets may be used or disclosed—for purposes of research, public health, or health care operations—without obtaining either an individual's authorization or a waiver or an alteration of authorization . There are two methods of determining whether a data set can be designated as a limited data set. Each is described below. A limited data set is covered by the minimum necessary standard.

Removal of Direct Identifiers

A limited data set may include city, state, zip code, elements of date, and other numbers, characteristics, or codes not listed as direct identifiers. Direct identifiers listed in the Privacy Rule's limited data set provisions apply both to information about the individual and to information about the individual's relatives, employers, or household members.

Of the 18 HIPAA PHI identifiers, two types are allowed in a limited data set:

1. Dates (in contrast to "Year" only)
2. Geographic information (in contrast to "state" only—but not street addresses)

In addition, limited data sets may contain unique identifying codes or numbers that are not specifically listed as PHI identifiers (See Re-identifying Codes).

Statistical Determination

A covered entity can also designate a data set as a limited data set if a statistical expert in the de-identification of data (a) determines that the risk of anyone being able to re-identify the data is very small and (b) documents the methods and results used to reach that conclusion.

Data Use Agreements

Data for a limited data set must be collected according to the terms of a data use agreement, which is "an agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected" (Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule). The data use agreement is the means by which a covered entity obtains satisfactory assurance that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes.

See a sample Data Use Agreement in this handbook or at www.uab.edu/irb/forms

The Data Use Agreement must contain the following information:

1. Identity of the person(s)/organization(s) to use or receive the data set;
2. Explanation of recipients' specific plans for use and/or disclosure;
3. Statement that recipient will protect the data from inappropriate use or disclosure;
4. Statement that the recipient will report use or disclosure not specified in the agreement;
5. Statement that the recipient's agents will protect the data from inappropriate use or disclosure; and
6. Statement that the recipient will not try to identify the PHI or contact the individuals.

Recruiting and Screening

HIPAA requires that recruitment techniques meet the standards for privacy and confidentiality. These guidelines describe four acceptable types of recruitment that should be followed after the protocol has been approved by the IRB.

1. Research recruitment by treating physicians/staff. Physicians and other health care providers may contact their own patients for purposes of recruiting them to participate in a research study.

    a. Treating physicians and staff within a division who work collaboratively to treat patients in clinic and who are also assigned to work on research protocols may review the clinic patients' records to identify potential research subjects for research protocols in which the division physicians are participating, provided the reviewer must agree that:
        (i) the sole purpose of the record review is to identify prospective research participants;
        (ii) the patient information to be reviewed is necessary to identify prospective participants for the study; and
        (iii) neither the patient records nor any patient-identifiable information will be copied or removed from the UAB/HSF/UABHS premises.

    b. After reviewing patient records to identify prospective research participants, treating physicians/staff may contact these patients to discuss the research opportunity.

2. Research recruitment by non-treating physicians/staff. Additional requirements must be met if physicians and other health care providers wish to contact patients other than their own for purposes of recruiting them to a research study.

    a. For a researcher and staff to review records or obtain lists of other physicians' patients, medical records, test results, or other clinical information when the researcher/staff is not involved in the treatment of the patients, the researcher/staff must include a description of the plan for recruitment in the IRB protocol submission, describe the method of contacting the individuals, and demonstrate the concurrence of the primary treating physician. In addition, consistent with UAB/UABHS/ HSF policies, the researcher/staff must agree that:
        (i) the sole purpose for obtaining the patient information is to identify prospective research participants;
        (ii) the patient information sought to be reviewed is necessary to identify prospective participants; and
        (iii) no patient-identifiable information will be copied or removed from the UAB/HSF premises.

b. IRB policy requires that any contact of possible recruits be done by the primary treating physician. However, in some instances, the IRB may approve contact by the researcher and the primary treating physician (i.e., joint letter) or by the researcher referencing the primary treating physician in the initial contact with the patient. Each protocol is reviewed by the IRB on a case-by-case basis to ensure that recruitment by researchers is done in a manner that does not inappropriately intrude on an individual's privacy.

3. Screening for eligibility. If screening potential research participants for eligibility in protocols involves soliciting health information from the participants, the researcher/staff must either (a) obtain a signed authorization from the participant prior to the screen or (b) request from the IRB a partial waiver of the authorization to allow the solicitation of health information for screening for eligibility into the protocol. (A sample request for partial waiver of the authorization to allow solicitation of health information for screening purposes can be found on the IRB web site).

4. Requesting that interested individuals contact the research staff. Researchers may continue to recruit individuals to participate in research protocols through IRB-approved advertisements, brochures, etc.

Recruiting without authorization or partial waiver is still allowed through the use of IRB-approved advertisements, brochures, and other means of public communications because such recruitment does not involve the use of PHI.

Regarding screening, if an investigator proposes a screening process that involves soliciting health information from the participants, then the investigator must either (a) obtain a signed authorization from the participant before the screen or (b) apply to the IRB for and receive a Partial Waiver of Authorization to allow the solicitation of health information during screening. Both forms are available at http://www.uab.edu/irb/forms.

Enforcement and Penalties

DHHS enforces civil monetary penalties for the HIPAA Standards, which became effective March 16, 2006. Civil penalties include fines up to $100 for each violation and up to $25,000 for identical violations during a calendar year. The U.S. Department of Justice is responsible for enforcing criminal penalties for the HIPAA Privacy Rule. Criminal penalties for "wrongful disclosure" include both fines of $50,000 to $250,000 and up to 10 years in prison. Examples of wrongful disclosures include accessing health information under false pretenses, releasing patient information with harmful intent, or selling the information.

Contacts

HIPAA Office	Shelia Searson	996-5051 ssearson@uab.edu
HIPAA Privacy Officer	Joan Hicks	934-4724 jhicks@uabmc.edu
HIPAA Security Officer	Terrell Herzig	975-0072 therzig@uab.edu
OIRB Director	Sheila Moore	934-3789 smoore@uab.edu
Legal Counsel	Kathleen Kauffman, J.D.	975-4844 kathleen@uab.edu

Resources

Office for Civil Rights "Base" Help Site

www.hhs.gov/ocr/hipaa/

Federal Regulations

45 CFR 46 (DHHS)

www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm#46.101

21 CFR 50 (FDA)

www.access.gpo.gov/nara/cfr/waisidx_00/21cfr50_00.html

21 CFR 56 (FDA)

www.access.gpo.gov/nara/cfr/waisidx_00/21cfr56_00.html

Federal Guidance Documents

Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule

privacyruleandresearch.nih.gov/pr_02.asp

HIPAA Guidance from OCR (Revised April 3, 2003)

General: www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf

Research: www.hhs.gov/ocr/hipaa/guidelines/research.pdf

UAB Policies and Guidance

UAB Health System Policies and Procedures and Forms

https://scr.hs.uab.edu/ (note *s* after *http*)

UAB Health System HIPAA Forms

www.health.uab.edu/

UAB IRB Guidebook and HIPAA Information

www.uab.edu/irb/guidebook/

www.uab.edu/irb/hipaa/

UAB/UABHS HIPAA Website
(containing UAB/UABHS HIPAA Core Standards, Forms, and other HIPAA-related Information)

www.hipaa.uab.edu

Glossary

Anonymized Data: See *De-identified Data*.

Authorization: An individual's written permission to allow a covered entity to use or disclose specified PHI for a particular purpose. Authorization may be waived by an IRB upon written request.

Confidentiality: Maintaining the secrecy of information (e.g., a medical record) whose unauthorized *disclosure* could be prejudicial to the subject of that information (e.g., a patient)

Covered Entity: A health plan, a health care clearinghouse, or a health care provider that transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard. UAB is a hybrid entity, meaning that it has functions both in *standard care* and in research.

Data Use Agreement: An agreement into which the covered entity enters with the intended recipient of a *limited data set* (LDS) that establishes the ways in which the information in the LDS may be used and how it will be protected.

De-identified Data: Data that do not contain any of the 18 identifiers listed in §164.514(b)(2)(i). Also known as de-identified data.

Designated Record Set (DRS): Individually identifiable data in any medium, collected and directly used by UABHS. The content may be in multiple locations and media, including paper and electronic form. The DRS consists of the Legal Medical Record and the Billing Record.

4.1.1. ***Legal Medical Record*:** The documentation of the health care services provided to an individual in any aspect of health care delivery by a health care provider organization used, in whole or in part, by or for the covered entity to make decisions about individuals.

4.1.2. ***Billing Record:*** The documentation in the billing records used, in whole or in part, by or for the covered entity to make decisions about individuals.

Disclosure: Any activity that allows individually identifiable health information to go **outside** the covered unit.

Health Information: Any information, oral or recorded, that (a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually Identifiable Health Information: A subset of health information, including demographic information collected from an individual, that identifies the individual or might reasonably be believed to make it possible to identify the individual.

Limited Data Set (LDS): Collected data that contains "PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's authorization or a waiver or an alteration of authorization for its use and disclosure, with a data use agreement" (Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule, p. 15).

Patient: A subject of treatment in a health care organization.

Participant: A living individual, about whom an investigator (whether professional or student) conducting research obtains (a) data through intervention or interaction with the individual, or (b) identifiable private information (referred to in federal regulations as a *human subject*).

Privacy: Being apart from company or observation.

Protected Health Information (PHI): Individually identifiable health information that is not covered by Family Educational Rights and Privacy Act (FERPA) or employment records.

Research: A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.

Re-identifying Code: A code or other mechanism used by a health care organization or other covered entity to allow its employees to restore identifying items to data that have been de-identified.

Standard Care: Medical or other care that meets generally accepted standards according to the condition of the patient (as opposed to care that involves a research component).

Use: The act of accessing individually identifiable health information for the purpose of clinical care **within** the covered unit.

University of Alabama at Birmingham

AUTHORIZATION FOR USE/DISCLOSURE OF HEALTH INFORMATION FOR RESEARCH

What is the purpose of this form? You are being asked to sign this form so that UAB may use and release your health information for research**.** Participation in research is voluntary. If you choose to participate in the research, you must sign this form so that your health information may be used for the research.

Participant Name: _____ **UAB IRB Protocol Number:** _____
Research Protocol: _____ **Principal Investigator:** _____
_____ **Sponsor:** _____
_____

What health information do the researchers want to use? All medical information and personal identifiers including past, present, and future history, examinations, laboratory results, imaging studies and reports and treatments of whatever kind related to or collected for use in the research protocol.

Why do the researchers want my health information? The researchers want to use your health information as part of the research protocol listed above and described to you in the Informed Consent document.

Who will disclose, use and/or receive my health information? The physicians, nurses and staff working on the research protocol (whether at UAB or elsewhere); other operating units of UAB, HSF, UAB Highlands, The Children's Hospital of Alabama, Callahan Eye Foundation Hospital and the Jefferson County Department of Public Health, as necessary for their operations; the IRB and its staff; the sponsor of the research and its employees; and outside regulatory agencies, such as the Food and Drug Administration.

How will my health information be protected once it is given to others? Your health information that is given to the study sponsor will remain private to the extent possible, even though the study sponsor is not required to follow the federal privacy laws. However, once your information is given to other organizations that are not required to follow federal privacy laws, we cannot assure that the information will remain protected.

How long will this Authorization last? Your authorization for the uses and disclosures described in this Authorization does not have an expiration date.

Can I cancel the Authorization? You may cancel this Authorization at any time by notifying the Director of the IRB, in writing, referencing the Research Protocol and IRB Protocol Number. If you cancel this Authorization, the study doctor and staff will not use any new health information for research. However, researchers may continue to use the health information that was provided before you cancelled your authorization.

Can I see my health information? You have a right to request to see your health information. However, to ensure the scientific integrity of the research, you will not be able to review the research information until after the research protocol has been completed.

Signature of participant: _____ Date: _____

or participant's legally authorized representative: _____ Date: _____

Printed name of participant's representative: _____

Relationship to the participant: _____

Data Use Agreement

This Data Use Agreement ("Agreement"), effective as of _____, 20___ ("Effective Date"), is entered into by and between _____ ("Recipient") and _____ ("Covered Entity"). The purpose of this Agreement is to provide Recipient with access to a Limited Data Set ("LDS") for use in its Research and Public Health analyses and for the Health Care Operations of the Covered Entity, in accord with the HIPAA Regulations.

1. Definitions. Unless otherwise specified in this Agreement, all capitalized terms used in this Agreement not otherwise defined have the meaning established for purposes of the "HIPAA Regulations" codified at Title 45 parts 160 through 164 of the United States Code of Federal Regulations, as amended from time to time.

2. Preparation of the LDS. Covered Entity shall prepare and furnish to Recipient a LDS in accord with the HIPAA Regulations or Covered Entity shall retain Recipient as a Business Associate (pursuant to an appropriate Business Associate Agreement) and direct recipient, as its Business Associate, to prepare such LDS.

3. Minimum Necessary Data Fields in the LDS. In preparing the LDS, Covered Entity or its Business Associate shall include the data fields specified by the parties from time to time, which are the minimum necessary to accomplish the purposes set forth in Section 5 of this Agreement.

4. Responsibilities of Recipient. Recipient agrees to:
    a. Use or disclose the LDS only as permitted by this Agreement or as required by law;
    b. Use appropriate safeguards to prevent use or disclosure of the LDS other than as permitted by this Agreement or required by law;
    c. Report to Covered Entity any use or disclosure of the LDS of which it becomes aware that is not permitted by this Agreement or required by law;
    d. Require any of its subcontractors or agents that receive or have access to the LDS to agree to the same restrictions and conditions on the use and/or disclosure of the LDS that apply to Recipient under this Agreement; and
    e. Not use the information in the LDS to identify or contact the individuals who are data subjects.

5. Permitted Uses and Disclosures of the LDS. Recipient may use and/or disclose the LDS for its Research and Public Health activities and the Health Care Operations of the Covered Entity.

6. Term and Termination.
    a. Term. The term of this Agreement shall commence as of the Effective Date and shall continue for so long as Recipient retains the LDS, unless sooner terminated as set forth in this Agreement.
    b. Termination by Recipient. Recipient may terminate this agreement at any time by notifying the Covered Entity and returning or destroying the LDS.
    c. Termination by Covered Entity. Covered Entity may terminate this agreement at any time by providing thirty (30) days prior written notice to Recipient.
    d. For Breach. Covered Entity shall provide written notice to Recipient within ten (10) days of any determination that Recipient has breached a material term of this Agree-

ment. Covered Entity shall afford Recipient an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to agree on mutually agreeable terms for cure within thirty (30) days shall be grounds for the immediate termination of this Agreement by Covered Entity.

e. Effect of Termination. Sections 1, 4, 5, 6(e) and 7 of this Agreement shall survive any termination of this Agreement under subsections c or d.

7. Miscellaneous.
   a. Change in Law. The parties agree to negotiate in good faith to amend this Agreement to comport with changes in federal law that materially alter either or both parties' obligations under this Agreement. Provided however, that if the parties are unable to agree to mutually acceptable amendment(s) by the compliance date of the change in applicable law or regulations, either Party may terminate this Agreement as provided in section 6.
   b. Construction of Terms. The terms of this Agreement shall be construed to give effect to applicable federal interpretative guidance regarding the HIPAA Regulations.
   c. No Third Party Beneficiaries. Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
   d. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.
   e. Headings. The headings and other captions in this Agreement are for convenience and reference only and shall not be used in interpreting, construing or enforcing any of the provisions of this Agreement.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

COVERED ENTITY	**RECIPIENT**
By: _____	By: _____
Print Name: _____	Print Name: _____
Print Title: _____	Print Title: _____