



HIPAA Privacy Compliance Plan for Research

University of South Alabama IRB Guidance and Procedures

**Office of Research Compliance and Assurance
CSAB 140
460-6625**

Adopted: 4/2/2003

HIPAA PRIVACY COMPLIANCE PLAN FOR RESEARCH
University of South Alabama

TABLE OF CONTENTS

I. INTRODUCTION

- A. Adoption of the HIPAA Privacy Compliance Plan**
- B. Purpose of the HIPAA Privacy Compliance Plan**

II. HIPAA PRIVACY COMPLIANCE POLICIES

Use and Disclosure Policies:

- A. Research Use of PHI With Authorization**
- B. Research Use of PHI Without Authorization**
 - 1. Waiver of Authorization
 - 2. Reviews Preparatory to Research
 - 3. Research on Decedent's Information
 - 4. Research Involving the Use of Limited Data Sets
- C. Use of De-Identified Data In Clinical Research**
- D. Transition Requirements**
- E. Research subjects' rights under HIPAA**
 - 1. Right to an accounting
 - 2. Right to revoke authorization
- F. Research Recruitment**
- G. Research Databases**

APPENDICES: HIPAA FORMS

- A. Waiver of Authorization**
- B. HIPAA Authorization Language (Template for HIPAA Portion of the Confidentiality Section of the Consent Form)**
- C. Revised Template for Confidentiality Section of the Consent Form**
- D. Investigator's Access Preparatory to Research**
- E. Research Involving Deceased Individuals**
- F. Limited Data Use Agreement**
- G. De-Identification Certification Form**

I. INTRODUCTION TO HIPAA

A. Adoption of the HIPAA Privacy Compliance Plan

The University of South Alabama is committed to complying with all local, state and federal laws relating to the privacy of health information and to consistently operate with the highest standards of business and professional ethics. In that regard, we have implemented this HIPAA Privacy Compliance Plan for Clinical Research to safeguard the confidentiality and privacy of protected health information (“PHI”) as required by the Federal Standards for Privacy and Individually Identifiable Health Information at 45 CFR Parts 160 and 164, subparts A and E, as may be amended and applicable state privacy laws.

The compliance date for health care facilities and providers is April 14, 2003. The regulations are commonly referred to as the “Privacy Rule” and are administered by the HHS Office of Civil Rights. The University of South Alabama as a whole is a “Hybrid Entity” which consists of a single entity whose business includes covered and non-covered functions. The covered functions are the health related components of the University: Hospitals, Diabetic Foot Clinic, Speech & Hearing Center, Psychology Clinic, and the USA Health Plan. The Covered Entities within the Hybrid Entity, along with the USA Health Services Foundation, are part of the USA Health System Organized Health Care Arrangement (OHCA). This means that within the OHCA different areas need to share protected health information about their patients, and that individuals who obtain services here expect that different areas share health information and are jointly managed.

By virtue of implementing and enforcing this Privacy Plan, we are committed to ensuring that PHI is collected, handled, transmitted and stored in a manner which preserves its confidentiality and privacy in accordance with the Privacy Rules. This guidance document serves as a primer that will focus only on HIPAA health data privacy regulations as they pertain to clinical research. Secondly, it is to provide a summary of revised IRB policies to fulfill the conditions set forth by the Privacy Rule in the research framework.

B. Purpose of the HIPAA Privacy Compliance Plan

This document is designed so that it is effective in preventing, detecting and remedying the improper use and disclosure of PHI at the University of South Alabama. The specific purposes of this Privacy Compliance Plan are:

- To assist us in identifying PHI and the manner in which it is to be used and disclosed;
- To assist us in avoiding improper use and disclosures of PHI;
- To establish compliance standards and procedures for members of our workforce;
- To effectively communicate the compliance standards, policies and procedures set forth in this Privacy Plan to all members who conduct clinical research;

- To take reasonable steps to achieve compliance with the standards, policies and procedures set for in this Privacy Plan by, for example, implementing, monitoring and auditing systems reasonably designed to detect the improper use and disclosure of PHI; and
- To respond appropriately to non-compliance after detection and to prevent recurrence, which may require modifications to this Privacy Plan.

The regulations impose three core requirements on health care providers and facilities (called “covered entities” in the regulatory text) that hold or maintain PHI. First, covered entities must obtain the agreement of patients to use or disclose their PHI unless specified exceptions are applicable. Secondly, persons must be notified by covered entities of their rights under the privacy regulations. Lastly, use and disclosure of PHI by covered entities must generally be restricted to the minimum necessary to accomplish the intended purpose. The Privacy Rule exercises four basic rights of persons with respect to their PHI to include: to agree to the use and disclosure of PHI, to inspect and copy their records, to amend their records and to obtain certain limited audits of the disclosures of their records that have been made by covered entities.

II. Research Use of PHI With Authorization

The HIPAA Privacy Rules characterize two basic types of written agreement that are utilized to secure the permission of persons for the use and disclosure of PHI. The first type is a general written consent by individuals for the use and disclosure of their PHI for treatment, payment and health care operations (“TPO”) in the non-research setting. This written consent provides a one-time blanket permission for a covered entity to use PHI for various purposes related to clinical care. The second type of written agreement involves authorization for the use of PHI for specific purposes other than TPO. Specific written authorization is required for the use and disclosure of PHI in research studies. Under the regulations, this authorization may be incorporated into consent forms for clinical research or may be secured via a separate authorization form. The University of South Alabama IRB Office has adopted the option of including the authorization in the consent form for research studies.

****** Core elements of information must be provided in writing to prospective subjects in securing authorization for the research use of their PHI. These items are provided in the HIPAA authorization template attached as Appendix B. This template must be inserted into the confidentiality section of the informed consent form. The revised template for the confidentiality section of the informed consent is attached as Appendix C.

A valid authorization for the release of PHI for research purposes requested by or asked of a potential subject in a research study must be retained for at least six years from the date permission is granted and must contain the following required elements: 1) a description of the information to be used or disclosed that identifies the information in a specific and meaningful manner; 2) the name of the covered entity or person(s) authorized to make the requested use or disclosure; 3) the name or other specific identification of the person(s) or entities which may include the covered entity itself to whom the covered entity may make the request for use or disclosure; 4) an expiration date and a signature and date; 5) the authorization must be written in plain language; 6) if the authorization is executed by a legal representative authorized to act for the individual, a description of his/her authority to act for the individual must be specified as

well as the relationship to the individual; 7) a statement that the individual acknowledges that he/she has the right to revoke the authorization except to the extent that information has already been disclosed under the authorization; 8) a statement that the individual acknowledges that information used or disclosed to any entity other than a health plan or health care provider may no longer be protected by the federal privacy law; 9) a description of the purpose(s) of the requested use or disclosure; 10) a statement that the individual may inspect or copy the protected health information to be used or disclosed; and 11) a statement that the individual may refuse to sign the authorization.

A. Research Use of PHI Without Authorization

HIPAA regulations allow the covered entity to use and disclose PHI for research purposes without subject authorization provided that any of the four criteria below are met. These include waiver of authorization, review of PHI preparatory to research, research involving a decedent’s information and use involving limited data sets. Applications for request to use PHI for research purposes without subject authorization should be submitted to the IRB. Without appropriate documentation and approval, PHI can only be disclosed with authorization from the individual.

1. Waiver of Authorization **

A covered entity is permitted to disclose PHI for research purposes without a written authorization when approval is obtained from the IRB. A waiver of authorization form is attached as Appendix A. In most cases, if a protocol will qualify for a waiver of a research informed consent from the IRB, it will be able to qualify for a waiver of authorization under HIPAA. The investigator must provide information about the research study that enables the IRB to determine that three requirements are satisfied:

- (1) there must be no more than minimal risk to the privacy of individual subjects based on the presence of the following elements:
 - an adequate plan to protect the identifiers from improper use and disclosure;
 - an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining identifiers or such retention is otherwise required by law;
 - an adequate written assurance that the PHI will not be reused or disclosed to any other person or entity, except as required by law, or for authorized oversight of the research study, or for other research for which the use or disclosure is permitted without authorization.
- (2) it must not be practicable to conduct the research without the waiver or alteration of the authorization requirement; and
- (3) it must not be practicable to conduct the research without access to and use of the PHI.

Once the IRB has approved the waiver of authorization, the investigator must provide the covered entity maintaining the PHI with documentation from the IRB of approval. The IRB approval letter will include the following elements:

1) identification of the IRB and provide the date on which the waiver of authorization was approved; 2) a statement that the IRB has determined that the waiver satisfies the criteria explained above; 3) provide a brief description of the PHI for which use or access has been determined to be necessary by the IRB; and 4) the letter must describe whether the request for waiver of the authorization requirements was reviewed via full board or expedited review procedures.

A waiver of authorization may be sought for three specific research uses of PHI to identify potential research subjects through review of their PHI, to contact potential subjects in order to determine their interest in research participation and to receive or collect PHI during the conduct of research studies.

** A waiver of authorization form is attached as Appendix A

2. Reviews Preparatory to Research **

Investigators may review PHI without authorization to prepare a research protocol or for similar purposes preparatory to research (i.e., limited to designing a study and/or determining the feasibility of completing a study). Neither recruitment nor patient contact is considered review preparatory to research. Under this provision of the regulations, the investigator must provide the following assurances to the covered entity:

1. The investigator shall not remove any protected health information from the covered entity;
2. The use/disclosure of PHI is sought solely for the purpose of preparing a research protocol; and
3. The PHI for which use or access is sought is necessary for research purposes.

In addition, reviews preparatory to research must not involve making copies of PHI or making notes that include PHI. However, medical records of interest to investigators in preparing a study may be flagged for future reference.

** Investigators may use PHI as preparatory to research if the investigator certifies the above provisions by completing the form attached as Appendix D.

3. Research on Decedent's Information **

A investigator is not normally required to submit research involving deceased individuals to the IRB for review, unless other living individuals such as family members could be affected (i.e., genetic markers of certain diseases) and should contact the IRB if assistance is needed to make this determination. If IRB review is necessary, the investigator shall submit a protocol to the IRB. If not, the investigator may use PHI of deceased individuals without authorization from the decedent's estate.

Qualifications under this provision requires that the researcher provide the covered entity:

1. Assurance that the use or disclosure is being sought solely for research on the PHI of decedents;
2. Documentation, at the request of the covered entity, of the death of such individuals; and
3. Assurance that the PHI is necessary for research purposes.

** Investigators may use PHI in research on decedent's information if the investigator certifies the above provisions by completing the form attached as Appendix E.

4. Research Involving the Use of Limited Data Sets **

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

- a) names
- b) postal address information, other than town or city, state and zip code
- c) telephone numbers
- d) fax numbers
- e) email addresses
- f) social security numbers
- g) health plan beneficiary numbers
- h) account numbers
- i) certificate/license numbers
- j) vehicle identifiers and serial numbers
- k) device identifiers and serial numbers
- l) web universal resources locators (URLs)
- m) Internet protocol (IP) address numbers
- n) biometric identifiers, including finger and voice prints
- o) full face photographic images and any comparable images
- p) A limited data set may, however include other indirect identifiers, especially dates of birth, treatment, discharge, or death.

** Investigators may use or disclose a limited data set without subject

authorization for research purposes only if a assurance is obtained in the form of a Limited Data Use Agreement attached as Appendix F.

C. Use of De-Identified Data in Clinical Research **

The de-identified health information under HIPAA is much more specific than the general de-identification standard applied under the federal laws relating to human research subjects. PHI can be released freely if it does not contain “individually identifiable information.” PHI is not individually identified if the subject is not identified, directly or indirectly, and has no reasonable basis to believe that the information can be used to identify the subject. It may be used in research without subject authorization or an IRB waiver. The Privacy Rule refers to such health information as “de-identified data.” Research which involves the use of “de-identified data” is exempt from the HIPAA requirements. To be exempt from HIPAA, none of the subject identifiers (see Appendix G) can be reviewed or recorded by the research team. In order to de-identify PHI, the investigator will comply with one of the two following procedures:

A. *Use of a Statistician to include:*

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

B. *Removal of all identifiers*

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

** For research involving de-identified health information the investigator shall complete the HIPAA De-identification Certification form in Appendix G. The IRB shall determine if the PHI has been adequately de-identified in accordance with the privacy laws. If so, the IRB shall issue documentation to the researcher confirming review and approval of the research protocol as involving de-identified health information. The investigator may then use the IRB approval notice to access and create a de-identified database.

D. Transition Provisions

Personnel at the University of South Alabama may continue to use and disclose information concerning a research subject for a particular study, without obtaining the HIPAA authorization or the IRB action required by this policy, regardless of when the information is created, collected or received, if, prior to April 14, 2003, the Principal Investigator obtained, and has written documentation of, any one of the following:

- An authorization or other express legal permission from the Research subject to use or disclose the Information for the Research study;
- The Research subject's informed consent to participate in the Research study;
- An IRB waiver of informed consent for the Research study.

If the investigator has such documentation for a research subject, he/she may create, collect, or receive information after April 14, 2003. However, for subjects without such written documentation prior to April 14, 2003, the investigator must obtain a specific authorization or other appropriate documentation required by this policy. For subjects who enroll in studies on or after April 14, 2003, the regulations of the Privacy Rule described above must be followed.

E. Research subjects' rights under HIPAA

1. Right to an accounting -

When a research subject signs an authorization to disclose PHI, the covered entity is not required to account for the authorized disclosure. Nor is an accounting required when the disclosed PHI is contained in a limited data set or is released to the researcher as de-identified data. However, an accounting is required for research disclosures of identifiable information obtained under a waiver or altered authorization, reviews preparatory to research and research on decedents. In general, the Privacy Rule requires that individuals have a right to receive an accounting of disclosures of PHI made by covered entities over a six year period. It is anticipated that requests for an accounting of disclosure will come to the hospitals and the medical records department will respond in accordance with the policy on HIPAA: Accounting of Disclosures.

2. Right to revoke authorization -

A research subject has the right to revoke his or her authorization unless the researcher has already acted in reliance on the original authorization. Under the authorization revocation provision, covered entities may continue to use or disclose PHI collected prior to the revocation as necessary to maintain the integrity of the research study. Examples of permitted disclosures include submissions of marketing applications to the FDA, reporting of adverse events, accounting of the subject's withdrawal from the study and investigation of scientific misconduct.

F. Research Recruitment

The Department of Health and Human Services states that covered entities may continue to discuss with patients the option of enrolling in a clinical trial. This can be done without subject authorization and without an IRB waiver of authorization. Similarly, direct care providers may communicate with their current or past patients about research opportunities without prior authorization of these patients. This permission does not extend, however, to disclosure of information to a third party for purposes of recruitment. In the latter case, the covered entity either has to obtain an authorization from the individual or secure a waiver of authorization as permitted by the Privacy Rule. The use of a partial waiver of authorization from the IRB would allow researchers to get specific information from other practitioners.

G. Research Databases

If a investigator maintains a database containing PHI, then the investigator has an obligation to insure that the use and disclosure of PHI is in compliance with HIPAA policies.

- A. Maintaining applicable security for the database, including physical security and access control;
- B. Control and manage the access, use and disclosure of PHI, including verifying appropriate IRB approvals and patient authorizations; and
- C. Any PHI in the database used for treatment or payment purposes must be a duplicate and the original must be included in the patient's medical record.

Remember, HIPAA applies to uses of PHI. In order to use a research database containing PHI, one must have authorization or a waiver from the IRB. Another pathway to using PHI in a research database is by utilizing a limited data set and completion of a Limited Data Use Agreement attached as Appendix F, enabling certain identifiers to be used during the research study. The users of a tissue bank database would need to obtain individual authorization or a IRB waiver if he/she wanted to use and disclose the information in a research study.



University of South Alabama

**REQUEST FOR WAIVER OR ALTERATION OF SUBJECT AUTHORIZATION
FOR THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION**

Project Title: _____

Investigator(s): _____

Department: _____ Contact #: _____

1. Check the activity for which the waiver or alteration of subject authorization is being requested:
 - Use of PHI for the conduct of the study itself
 - Use of PHI to identify potential subjects for recruitment
 - Use of PHI to contact potential subjects regarding study participation
2. If an alteration of authorization is being requested, briefly describe the proposed alteration of the authorization and attach a copy of the altered authorization section of the consent form. If a waiver is being requested proceed to number 3.
3. The following protected health information will be created, collected, used or disclosed as a result of the subject's participation in this research:

4. There is minimal risk to the privacy of the subject because:
 - a. State how the PHI will be protected from improper use and disclosure. (i.e., the information will not be disclosed unless it is stripped of all identifiers, Data will be coded prior to any disclosure with P.I. retaining a master list with a code access)

 - b. Identifiers will be destroyed upon completion of :
 - Data collection
 - Data analysis
 - Specimen processing
 - Other : _____

- OR -

- c. Identifiers will be retained indefinitely because:
 - This is a longitudinal study
 - Of federal requirements
 - Other: _____
5. The research cannot practicably be conducted without access to the PHI because:
 - PHI is needed to identify subject eligibility
 - Explain: _____
 - PHI is needed to answer the research question
 - Explain: _____
 - _____
 - Other: _____

- 6. List all entities (i.e., USA), organizations and/or persons involved in the use and disclosure of the PHI.

(Note: If the identifiable health information is shared outside of USA, additional documentation may be necessary to account for the disclosure(s). Furthermore, the sharing of PHI outside of USA may require the outside party to comply with HIPAA requirements.)

The information listed in the waiver application is accurate and all research staff will comply with the HIPAA regulations and the waiver criteria. I assure that the information I obtain as part of this research will not be reused or disclosed to any person or entity other than those listed on this form, except as required by law.

Principal Investigator

Date

<u>For IRB Use Only</u>	
This waiver was approved under: Full Review _____ Expedited review _____	
_____ Signature of IRB Chair or Designee	_____ Approval Date

APPENDIX B

AUTHORIZATION TO USE AND DISCLOSE INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION IN CLINICAL RESEARCH

Template: **HIPAA Portion of the Confidentiality Section of the Consent Form**

PLEASE NOTE:

**The authorization language provided below should be inserted at the appropriate location in the confidentiality section of the consent form. (Refer to revised template for Confidentiality Section)
The language in the template should be directly followed.**

Study records that identify you will be kept confidential as required by law. Under federal privacy regulations, you have the right to determine who has access to your personal health information (called “PHI”) which provides safeguards for privacy, security and authorized access. PHI collected in this study may include **[INSERT SPECIFIC CRITERIA AS IT RELATES TO YOUR PROTOCOL – Examples to include:** your medical history, results of physicals exams, lab tests, x-ray exams, other diagnostics and treatment procedures, as well as basic demographic information.] In addition to the investigator(s) listed on the last page of this consent form and their research staff, the following individuals will or may have access to identifiable information related to your participation in this research study. A representative of the University of South Alabama Research Compliance and Assurance Office may review your PHI for the purpose of monitoring the appropriate conduct of this research study. **[Remove the following sentence if not applicable to your protocol -** Reviewers may also include representatives from the Food and Drug Administration for the purpose of monitoring the accuracy of the research data, University of South Alabama Health System, legal counsel, and your medical insurance carrier.] The University of South Alabama Institutional Review Board may review your PHI as part of its responsibility to protect the rights and welfare of research subjects. **[Remove the following two sentences if not applicable to your protocol -** PHI may also be shared with the sponsor of this study, **(INSERT SPONSOR)**, for the purpose of monitoring the accuracy and completeness of the research data and performing required scientific analyses of the research data. The investigator(s) involved in the conduct of this research may receive funding from the sponsor to perform the research procedures and to provide the sponsor with identifiable research information related to your participation]. Your PHI will not be used or disclosed to any other person or entity, except as required by law, or for authorized oversight of this research study by other regulatory agencies, or for other research for which your PHI has been approved by the Institutional Review Board. Please be aware that once PHI is disclosed, there is the possibility that your personal health information may no longer be protected by applicable privacy laws and regulations.

The study results will be retained in your research record for a minimum of six years or until after the study is completed, whichever is longer. At that time either the research information not already in your medical record will be destroyed or information identifying you will be removed from such study results. Any research information obtained in your medical record will be kept indefinitely.

This authorization does not expire. At anytime, you may cancel this authorization in writing by contacting the principal investigator listed on the first page of the consent form. If you refuse to provide this authorization, you will not be able to participate in the research study. If you cancel the authorization, then you will be withdrawn from the study. However, information gathered before the cancellation date may be used if necessary in completing the research study or any follow-up for this study. **[Remove the following sentence if protocol is a non-clinical study]** - In accordance with the USA Health System Privacy Notice document, you are permitted to obtain access to your PHI collected or used in this study. Such access will be granted at the end of the study.

APPENDIX C

Revised Template: For the Confidentiality Section of the Consent Form

CONFIDENTIALITY:

1. Provide a statement explaining how individual identifiers will be used in maintaining the research records (i.e., research record labeled with subject's name or research records labeled with a code number. A master key that links the name and code number will be maintained in a separate and secure location).
2. Insert HIPAA authorization portion in confidentiality section. (refer to HIPAA authorization language template)
3. If the study involves the use of a federal Certificate of Confidentiality, provide the information about the certificate and how it protects subject information from re-disclosure. *(Example: To further help protect your privacy, the investigators have obtained a confidentiality Certificate from the U.S. Department of Health and Human Services (DHHS). With this federal Certificate, the investigators cannot be forced (i.e., court order) to disclose information that may identify you in any federal, state or local court. However, disclosure is necessary upon the request of the DHHS (i.e., for audit or program evaluation).*
4. If information about the subject's participation in the study or the results of procedures performed in the study will be placed in the subject's medical record (as contrasted with research record), then it should be specified.
5. Specify that the individual subjects will not be identified in any presentations or publications based on the results of the research study.



APPENDIX D

University of South Alabama

INVESTIGATOR’S ACCESS PREPARATORY TO RESEARCH

Assurances under this provision of the HIPAA Privacy Rule requires investigators who intend to perform a review preparatory to research make certain representations before using or disclosing protected health information in such a review. “Use” is sharing PHI within the USA entity. A “disclosure” is sharing PHI with someone outside the USA entity.

The investigator must complete this form and submit to the IRB Office, CSAB 138. A IRB letter of approval will be issued for reviews preparatory to research. The investigator should provide this assurance to medical records or the entity to receive such information in order to access the records/PHI.

I, _____, will adhere to the following representations:

1. I will not remove any protected health information from the covered entity;
2. The use/disclosure of PHI is sought solely for the purposes to prepare a research protocol; and
3. The PHI for which use or access is sought is necessary for research purposes
4. If I record any PHI, it will not include patient names, medical record numbers, social security numbers or patient account numbers.
5. The minimum necessary PHI to accomplish my work is:

Research staff needing access to protected health information:

Principal Investigator

Date

<p>Date received by IRB :</p>



University of South Alabama

APPENDIX E

RESEARCH INVOLVING DECEASED INDIVIDUALS

Assurances under this provision of the HIPAA Privacy Rule requires investigators who intend to conduct research involving decedent's information must make certain representations before using or disclosing decedent's protected health information for research. "Use" is sharing PHI within the USA entity. A "disclosure" is sharing PHI with someone outside the USA entity.

I, _____, intend to examine records/specimens of deceased individuals that contain PHI and will adhere to the following representations:

1. The research requires the review of PHI solely for research on deceased individuals.
2. The access sought to PHI is necessary for research purposes.
3. If requested, I will provide documentation of the death of the individual(s) whose protected health information that will be accessed.

Research staff needing access to protected health information:

Signature of Principal Investigator

Date

Please note: the covered entity from which you request the protected health information may request documentation of death.

IRB review is not necessary for research involving deceased individuals. However, if you will be maintaining health information linked to identifiers that could affect family members of the deceased (i.e., genetic makers of certain diseases), you may have to submit the research to the IRB. In that case, you will not need to submit this form.

Date Received by IRB:

APPENDIX F LIMITED DATA USE AGREEMENT

THIS LIMITED DATA USE AGREEMENT ("LDU Agreement") is made and entered into as of this ____ day of _____, _____ (the "Effective Date") by and between University of South Alabama Hospitals (hereinafter referred to as the "Covered Entity") and _____ (hereinafter referred to as the "Recipient").

WHEREAS, Recipient desires to obtain certain information from Covered Entity for the limited purposes of performing Recipient (i) Research; (ii) Public Health Activities; or (iii) Health Care Operations and, in connection with those purposes, Recipient will receive from Covered Entity certain Protected Health Information in the form of a Limited Data Set ("LDS") that is subject to protection under the Privacy Rules of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA");

WHEREAS, Covered Entity and Recipient intend to protect the privacy and provide for the security of the LDS in compliance with the Privacy Rules; and

WHEREAS, the Privacy Rules require Recipient to enter into a contract containing specific requirements that it must meet in order to receive the LDS from or on behalf of Covered Entity.

NOW, THEREFORE, in consideration of the foregoing and of the covenants and agreements set forth herein, the parties, intending to be legally bound, agree as follows:

Section 1. Definitions. The terms used, but otherwise not defined, in this LDU Agreement shall have the same meaning as those terms in the Privacy Rules.

(a) "Recipient" shall mean the person or entity designated as such above, as well as his/her/its officers, directors, employees, agents and representatives.

(b) "Health Care Operations" shall have the meaning set forth in 45 CFR 164.501, including, without limitation, the following activities of Recipient: quality assessment and improvement activities, credentialing, accreditation, conducting medical reviews, legal services, business planning and development, business management, and general administrative activities.

(c) "Individual(s)" shall have the meaning set forth in 45 CFR 164.501, including, without limitation, a person who is the subject of the LDS, and shall include an individual or entity who qualifies as a personal, legal representative of the person, as the context requires.

(d) "Limited Data Set" ("LDS") shall mean Protected Health Information that Recipient receives from, or on behalf of, Covered Entity and that excludes the following direct identifiers of the Individual and of relatives, employers or household members of the Individual pursuant to 45 CFR 164.514(e): names; postal address information (other than town or city, state and zip code); telephone and fax numbers; e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers (including license plate); device identifiers and serial numbers; web universal resource locators (URLs); internal protocol (IP) address numbers; and biometric identifiers, including finger and voice prints and full face photographic images and any comparable images.

(e) "Privacy Rules" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, Subparts A and E, as may be amended, modified or superceded, from time to time.

(f) "Protected Health Information" shall have the meaning set forth in 45 CFR 164.501, including, without limitation, any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; or (ii) the provision of health care to an individual; or (iii) the

past, present or future payment for the provision of health care to an individual; and (iv) 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.

(g) "Required by Law" shall have the meaning set forth in 45 CFR 164.501, including, without limitation, a mandate contained in law that compels a covered entity to make a use or disclosure of PHI and that is enforceable in a court of law.

(h) "Public Health Activities" shall have the meaning set forth in 45 CFR 164.512(b), including, without limitation: (i) a public health authority that is authorized by law to collect or receive Protected Health Information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, the reporting of disease, injury, vital events such as birth and death, and the conduct of public surveillance or public health investigations; (ii) a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect; (iii) a person subject to the jurisdiction of the Food and Drug Administration ("FDA") with respect to an FDA-regulated product or activity for which that person has responsibility; or (iv) a public health authority that is authorized by law to notify a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition.

(i) "Research" shall have the meaning set forth in 45 CFR 164.501, including, without limitation, a systematic investigation, including research development, testing, and evaluation, designated to develop or contribute to generalizable knowledge.

(j) "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his/her designee.

Section 2. Obligations of Recipient.

(a) Limited Data Set. Recipient shall have access only to the following specific LDS information; as set forth in Section 1(d): _____
_____. Recipient hereby affirms and acknowledges that his/her/its request for LDS information is the minimum necessary to accomplish his/her/its purpose as set forth in Section 2(b) below.

(b) Permitted Uses. Recipient shall not use LDS except for the express purpose of performing Recipient's (note: specifically describe the particular Research, Public Health Activity or Health Care Operation purpose): _____
_____. Recipient shall not use the LDS in any manner that would constitute a violation of the Privacy Rules.

(c) Permitted Disclosures. Recipient shall not disclose LDS except as may be related to the specific purpose(s) as set forth in § 2(b) and shall not disclose LDS in any manner that would constitute a violation of the Privacy Rules.

(d) Appropriate Safeguards. Recipient shall implement appropriate administrative, technical and physical safeguards in compliance with the Privacy Rules as are necessary to prevent the use and/or disclosure of LDS other than as permitted by the terms of this LDU Agreement. Recipient shall maintain a comprehensive written information privacy program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Recipient's operations and the nature and scope of his/her/its activities in order to safeguard the LDS.

(e) Recipient's Agents and/or Subcontractors. To the extent Recipient retains any agents or subcontractors that will use or have access to the LDS for the purposes of performing Recipient's (i) Research; (ii) Public Health Activities; or (iii) Health Care Operations in accordance with Exhibit A, Recipient shall require that each agent or

subcontractor agree, in writing, to be bound by the terms of this LDU Agreement to the same extent as Recipient. Recipient shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation.

(f) Re-Identify or Contact Individuals. The Recipient agrees not to re-identify or contact the Individual(s) who is/are the subject(s) of the LDS.

(g) Governmental Access to Records. Recipient shall make his/her/its internal practices, books and records relating to the use and disclosure of LDS available to Secretary in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rules. Recipient shall provide Covered Entity access to or a copy of any LDS or other information that Recipient makes available to the Secretary concurrently with providing such LDS to the Secretary.

(h) Covered Entity Access to Records. Within five (5) days of a written request by Covered Entity, Recipient shall allow Covered Entity to conduct a reasonable inspection of Recipient's facilities, systems, books, records, agreements, policies and procedures relating to the use and/or disclosure of LDS for the purpose of determining whether Recipient has complied with this LDU Agreement; provided, however, that: (i) Recipient and Covered Entity shall mutually agree in advance upon the scope, timing and location of such an inspection; (ii) Covered Entity shall protect the confidentiality of all confidential and proprietary information of Recipient to which Covered Entity has access during the course of such inspection; and (iii) Covered Entity shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Recipient. The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Recipient's facilities, systems, books, records, agreements, policies, and procedures does not relieve Recipient of his/her/its responsibility to comply with this LDU Agreement. Moreover, Covered Entity's failure to detect or, in the alternative, detection, but failure to notify or require Recipient to remediate any unsatisfactory practices, does not constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under this LDU Agreement.

(i) Minimum Necessary Use and Disclosure Requirement. Recipient shall only request, use or disclose the minimum amount of LDS necessary to reasonably accomplish the purpose of the request, use or disclosure in accordance with 45 CFR 164.502(b). Further, Recipient will restrict access to LDS to those employees of Recipient or other workforce members under control of Recipient who are actively and directly participating in the request, use or disclosure of LDS in accordance with the purposes set forth in Exhibit A and who need to know such information in order to fulfill such responsibilities.

(j) LDS Ownership. Recipient acknowledges that it has no ownership rights with respect to LDS received by Recipient pursuant to this LDU Agreement.

(k) Notification of Breach; Mitigation. During the term of this LDU Agreement, Recipient shall notify Covered Entity within twenty-four (24) hours of any actual or suspected use and/or disclosure of LDS in violation of the Privacy Rules or this LDU Agreement. Recipient shall take prompt corrective action to mitigate and cure any harmful effect that is known to Recipient of an improper use and/or disclosure of LDS.

Section 3. Term and Termination.

(a) **Term.** This LDU Agreement shall commence on the Effective Date and will remain effective for the entire time Recipient maintains the LDS, unless earlier terminated in accordance with the terms herein.

(b) **For Cause Termination Due to Material Breach.** In the event of a material breach by Recipient of any of his/her/its obligations hereunder, Covered Entity shall have the right, as specifically recognized by Recipient, to terminate this LDU Agreement at any time by providing Recipient written notice of termination setting forth a description of the breach and the effective date of termination.

(c) **Reasonable Steps to Cure Material Breach.** If Covered Entity knows of a pattern of activity or practice of Recipient that constitutes a material breach of Recipient's obligations under the provisions of this LDU Agreement and does not terminate this LDU Agreement pursuant to Section 3(b) above, then Recipient shall take reasonable steps to cure such breach. If Recipient's efforts to cure such breach are unsuccessful within thirty (30) days following a written request to cure provided by Covered Entity, Covered Entity shall either: (i) terminate this LDU Agreement, if feasible; or (ii) if termination of this LDU Agreement is not feasible, Covered Entity shall report Recipient's breach to the Secretary.

(d) **Judicial or Administrative Proceedings.** Either party may terminate this LDU Agreement, effective immediately, if: (i) the other party is named as a defendant in a criminal proceeding for a violation of the Privacy Rules; or (ii) there is a finding or stipulation that the other party has violated any standard or requirement of the Privacy Rules in any administrative or civil proceeding.

(e) **Effect of Termination.** As of the effective date of termination of this LDU Agreement, neither party shall have any further rights or obligations hereunder except: (a) as otherwise provided herein; (b) for continuing rights and obligations accruing under the Privacy Rules; or (c) arising as a result of any breach of this LDU Agreement, including, but not limited to, any rights and remedies available at law or equity. Upon termination of this LDU Agreement for any reason, Recipient shall return or destroy all LDS (regardless of form or medium), including all copies thereof. The obligation to return or destroy all LDS shall also apply to LDS that is in the possession of agents or subcontractors of Recipient. If the return or destruction of LDS is not feasible, Recipient shall provide Covered Entity written notification of the conditions that make return or destruction not feasible. Upon mutual agreement of the parties that return or destruction of LDS is not feasible, Recipient shall continue to extend the protections of this LDU Agreement to such information, and limit further uses or disclosures of such LDU to those purposes that make the return or destruction of such LDU not feasible, for as long as Recipient maintains such LDU. If Recipient elects to destroy the LDU, Recipient shall notify Covered Entity in writing that such LDU has been destroyed.

Section 4. Indemnification. Recipient shall indemnify and hold the Covered Entity, and its employees, officers, directors and independent contractors, harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards or other expenses, of any kind or nature whatsoever, including, without limitation, attorneys' fees, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any breach or alleged breach of this LDU Agreement by Recipient. The obligations set forth in this Section 5 shall survive termination of this LDU Agreement, regardless of the reasons for termination.

Section 5. Disclaimer. Covered Entity makes no warranty or representation that compliance by Recipient with this LDU Agreement or the Privacy Rules will be adequate or satisfactory for Recipient's own purposes. Recipient is solely responsible for all decisions made by Recipient regarding the safeguarding of its confidential information.

Section 6. Assistance in Litigation or Administrative Proceedings. Recipient shall be available to Covered Entity, at no cost to Covered Entity, to testify as a witness, or otherwise provide reasonable assistance, in the event of litigation or administrative proceedings being commenced against Covered Entity, his/her/its directors, officers or employees based upon a claimed violation of HIPAA, the Privacy Rules or other laws relating to LDS security or privacy, except where Recipient is named as an adverse party.

Section 7. Injunctive Relief. In the event of a breach by Recipient of any of his/her/its obligations hereunder, Covered Entity shall have, in addition to any other rights and remedies available at law or in equity, the right to obtain injunctive relief without the necessity of proving actual damages or that any irreparable harm would or might result from a failure to obtain injunctive relief, it being acknowledged and agreed to by all parties hereto that any such breach will cause irreparable harm to Covered Entity and that monetary damages alone will not provide an adequate remedy.

Section 8. Construction. This LDU Agreement shall be construed as broadly as necessary to implement and comply with the Privacy Rules. The parties agree that any ambiguity in this LDU Agreement shall be resolved in favor of a meaning that complies and is consistent with the Privacy Rules.

Section 9. Captions. The captions contained in this LDU Agreement are included only for convenience of reference and do not define, limit, explain or modify this LDU Agreement or its interpretation, construction or meaning and are in no way to be construed as part of this LDU Agreement.

Section 10. Notice. All notices and other communications required or permitted pursuant to this LDU Agreement shall be in writing, addressed to the party at the address set forth at the end of this LDU Agreement, or to such other address as either party may designate from time to time in writing in accordance with this Section. All notices and other communications shall be mailed by registered or certified mail, return receipt requested, postage pre-paid; by facsimile with a copy sent by First Class Mail, postage prepaid; or transmitted by hand delivery. All notices shall be effective as of the date of delivery by hand delivery, two (2) days following the date of facsimile, or for certified mail on the date of receipt, whichever is applicable.

Section 11. Assignment. This LDU Agreement and the rights and obligations hereunder shall not be assigned, delegated, or otherwise transferred without the prior written consent of the other party and any attempted assignment or transfer without proper consent shall be null and void.

Section 12. Governing Law and Venue. This LDU Agreement shall be governed by, and interpreted in accordance with, the Privacy Rules and the laws of the State of Alabama, without giving effect to any conflict of laws provisions. Any action at law, suit in equity, or other judicial proceeding for the enforcement of this LDU Agreement, or any provision hereof, shall take place in the State of Alabama in the County in which Covered Entity has his/her/its place of business. Recipient hereby consents to the personal jurisdiction of the state and federal courts in such County, in any dispute arising from or related to this LDU Agreement.

Section 13. Binding Effect; Modification. This LDU Agreement shall be binding upon, and shall enure to the benefit of, the parties hereto and their respective permitted successors and assigns. This LDU Agreement may only be amended or modified by mutual written agreement of the parties; provided, however, that in the event provisions of this LDU Agreement shall conflict with the requirements of the Privacy Rules, this LDU Agreement shall automatically be deemed amended as necessary to comply with such legal requirements.

Section 14. Waiver. The failure of either party at any time to enforce any right or remedy available hereunder with respect to any breach or failure shall not be construed to be a waiver of such right or remedy with respect to any other breach or failure by the other party.

Section 15. Severability. In the event that any provision or part of this LDU Agreement is found to be totally or partially invalid, illegal, or unenforceable, then the provision will be deemed to be modified or restricted to the extent and in the manner necessary to make it valid, legal, or enforceable, or it will be excised without affecting any other provision of this LDU Agreement with the parties agreeing that the remaining provisions are to be deemed to be in full force and effect as if they had been executed by both parties subsequent to the expungement of the invalid provision.

Section 16. No Third-Party Beneficiaries. Nothing express or implied in this LDU Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Recipient and their respective successors or permitted assigns, any rights, remedies, obligations or liabilities whatsoever.

Section 17. Entire Agreement. This LDU Agreement constitutes the entire agreement between the parties with respect to the matters contemplated herein and supersedes all previous and contemporaneous oral and written negotiations, commitments, and understandings relating thereto.

[Signatures on the following page.]

IN WITNESS WHEREOF, Covered Entity and Recipient have each caused this LDU Agreement to be executed in their respective names by their duly authorized representatives, as of the day and year first above written.

"COVERED ENTITY"

"RECIPIENT"

University of South Alabama Hospitals

Signature: _____

Signature: _____

Print Name: _____

Print Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Address: _____

Address: _____

Facsimile: _____

Facsimile: _____



APPENDIX G

University of South Alabama DE-IDENTIFICATION CERTIFICATION FORM

Do not complete if Authorization will be obtained or Waiver of Authorization is requested.

IRB Protocol: _____ P.I. Name: _____

Title: _____

I certify that the protected health information (PHI) received or reviewed by research personnel for the research study referenced above does not include any of the 18 identifiers listed below. Also, all research staff involved with the study has or will become familiar with the University of South Alabama HIPAA Privacy Compliance Plan for Research.

1. Names (individual, employer, relatives, etc.)
2. Address (street, city, county, zip code- initial 3 digits if geographic unit contains less than 20K people, or any other geographical codes)
3. Telephone numbers
4. Fax numbers
5. Social Security numbers
6. All elements of dates (except for years)
 - Birth Date
 - Admission Date
 - Discharge Date
 - Date of Death
 - Ages > 89 and all elements of dates indicative of such age
7. E-mail addresses
8. Web Universal Resource Locator (URL's)
9. Internet Protocol (IP) address numbers
10. Medical Record numbers
11. Health Plan Beneficiary Numbers
12. Account Numbers
13. Certificate/License Numbers
14. Vehicle Identifiers and Serial Numbers (e.g., VINs, License Plate Numbers)
15. Device Identifiers and Serial Numbers
16. Biometric Identifiers
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

Principal Investigator

Date

PHI = individually identifiable health information transmitted or maintained in any form (electronic means, on paper or through oral communication) that relates to the past, present or future physical or mental health or conditions of an individual.