

Use of Personal Health Information under the Health Insurance Portability and Accountability Act (HIPAA)

Last Revision Wednesday, January 31st, 2007
11:30:14 AM Central Standard Time

1. Introduction
2. Personal Health Information and Research under HIPAA
 1. Written Individual Authorization
 2. De-identification
 3. Limited Data Sets
 4. Reviews Preparatory to Research
 5. Waiver of Individual Authorization
 6. Research on Decedents
 7. Related Issues
 1. Notifying Research Subjects of their Privacy Rights
 2. Research Recruitment under HIPAA
 3. Research Repositories
 4. "Minimum Necessary" Standard and Role-Based Access
 5. Transition Requirements for Ongoing Research
 6. Accounting for Research Disclosure
3. Business Associates under HIPAA
 1. Who May Qualify as a Business Associate
 2. Use of Data by a Business Associate for Separate Research Purposes
 1. De-identified Data
 2. The Limited Data Set Alternative
 3. Standard Business Associate Agreement Provisions: What They Require
 4. Steps to Take as a Project Director
4. HIPAA-Related Forms and Templates

i) Introduction

The "Privacy Rule" and its companion regulation, the "Security Rule," are Federal Regulations under the [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#). By law, they apply to "Covered Entities"-health plans, health care clearinghouses, and health care providers. The Privacy and Security Rules directly regulate the way Covered Entities handle individually identifiable health information known as "protected health information" or "PHI." These regulations impact researchers and others working with or for Covered Entities because they restrict the ability of Covered Entities to use and disclose PHI, and, by extension, the ability of researchers to use PHI for research purposes. Generally speaking, PHI includes individually identifiable health, demographic, and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse, regardless of format, held or maintained by a Covered Entity or "Business Associates" acting on behalf of the Covered Entity. It does not include individually identifiable health information maintained in education records covered by the Family Educational Right and Privacy Act (as amended, 20 U.S.C. 1232g) and records described at 20 U.S.C. 1232g(a)(4)B(iv), or employment records held by a Covered Entity in its role as an employer. The Privacy Rule does not protect individually identifiable health information that is held or maintained by entities other than Covered Entities.

The Privacy Rule permits a Covered Entity to assign to, and retain with, the health information a code or other means of record identification if that code is not derived from or related to the information about the individual and could not be translated to identify the individual. The Covered Entity may not use or disclose the code or other means of record identification for any other purpose and may not disclose its method of re-identifying the information. For example, a Covered Entity could randomly assign a code that could be re-identified through a secured key not related to the information about its assigned PHI, because a random code would not be derived from or related to information about the individual and because the key to that code would be secure.

Information regarding HIPAA's requirements for the use and disclosure of PHI in the contexts of (a) research and (b) the provision of services to Covered Entities by Business Associates is set forth below. The following specific topics are covered:

Note: Other state and federal laws may apply to a particular use and disclosure of health information, even in cases where HIPAA also applies. For example, the Privacy Rule will not override a state law that is more stringent in its protection of individually identifiable health information than the Privacy Rule. Also, the standards of a particular Covered Entity or KU's Institutional Review Board (IRB), the [Human Subject Committee-Lawrence Campus \(HSCL\)](#), may be more restrictive than the Privacy Rule in some cases. All research and related activities must be reviewed and approved in accordance with university policies and procedures. The [HIPAA Tutorial](#) also includes information about how HIPAA applies to research.

ii) Personal Health Information and Research under HIPAA

HIPAA outlines the conditions under which a Covered Entity may use or disclose PHI for research purposes. HIPAA defines "research" as a systematic investigation, including research development, testing and evaluation, **designed to develop or contribute to generalizable knowledge**.

Under HIPAA, a Covered Entity may not use or disclose PHI for research unless the subject of the information has granted permission via a written Authorization form, **OR** one of the following criteria is met:

- the information is completely "De-identified";
- the information is compiled into a "Limited Data Set" and a Data Use Agreement is executed;
- the activity qualifies as "preparatory to research";
- a waiver of the individual Authorization requirement is obtained from an Institutional Review Board (IRB) or Privacy Board; or
- the researcher is accessing information solely on decedents.

Researchers must ensure that these requirements are met when engaging in research involving PHI. These requirements are addressed in more detail below.

(a) Written Individual Authorization

As stated above, written authorization from the patient/research subject is the default requirement for use or disclosure of that individual's PHI in research. The authorization must be written in plain language and it must be study specific. It must contain the following elements:

- A specific description of the PHI to be used or disclosed.
- The names or other specific identification of the person(s) or classes of person(s) authorized to make the use or disclosure;
- The names or other specific identification of the person(s) or classes of person(s) authorized to receive the use or disclosure;
- A description of each purpose of the requested use or disclosure;
- An expiration date or event for the Authorization that relates to the individual or to the purpose of the use or disclosure. The statement "end of the research study," "none" or similar language is sufficient if the authorization is for research, including for the creation and maintenance of a research database or repository;
- A statement that the individual has a right to revoke the authorization and how to do so, and, if applicable, the exceptions to the right to revoke;
- A statement regarding whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on the authorization, including research-related treatment and consequences of refusing to sign, if applicable;
- A statement of the potential risk that PHI will be redisclosed by the recipient and no longer protected by the Privacy Rule;
- The signature of the individual and date. (If signed by a personal representative, a description of the representative's authority to act for the individual must also be provided.)

The research subject must receive a copy of the signed authorization. In addition, research subjects may revoke their privacy authorization at any time during the research. If permission is revoked, HIPAA allows continued use and disclosure of the information that was obtained prior to the revocation in order to preserve the integrity of the study. For example, the researcher may use the information to account for study withdrawals, to report adverse events to the FDA, or to comply with study audits.

Under HIPAA, the required authorization elements may be included in a separate document or incorporated into the confidentiality section of the consent document for the same research. HSCL's example consent form on the HSCL Forms & Policies page incorporates the HIPAA authorization elements. Proposed privacy authorization language must be included with the HSCL application.

(b) De-identification

Certain research projects can be accomplished through the use of de-identified data. Covered Entities may use or disclose health information that is "de-identified" without restriction under the Privacy Rule.

Information may be de-identified in one of two ways. Under the **first method**, the Covered Entity must remove from each record the following eighteen elements that could be used to identify an individual or an individual's relatives, employers, or household members:

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
 1. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
 2. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Full-face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

A de-identified data set might include age, gender, ethnicity, marital status and relevant medical information, provided there are no identifying links to the source data.

The Privacy Rule permits a Covered Entity to assign to, and retain with, the health information a code or other means of record identification if that code is not derived from or related to the information about the individual and could not be translated to identify the individual. The Covered Entity may not use or disclose the code or other means of record identification for any other purpose and may not disclose its method of re-identifying the information. For example, a randomly assigned code that permits re-identification through a secured key to that code would not make the information to which it is assigned PHI, because a random code would not be derived from or related to information about the individual and because the key to that code is secure.

The **second method** of de-identification involves the use of statistical methods instead of the removal of all eighteen identifiers. 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" that there is a "very small" risk that the information could be used by the recipient to identify the individual who is the subject of the information, alone or in combination with other reasonably available information. The person certifying statistical de-identification must document the methods used

as well as the result of the analysis that justifies the determination. A Covered Entity is required to keep such certification, in written or electronic format, for at least six years from the date of its creation or the date when it was last in effect, whichever is later.

For a researcher to view a Covered Entity's records containing PHI and from those records extract a de-identified data set, one of the Privacy Rule's conditions for disclosure of the PHI to the researcher must be met, for example receipt of individual authorization or waiver of the individual authorization requirement from an IRB or Privacy Board. Alternatively, in some cases, the Covered Entity may be able to enter into a "Business Associate Agreement" with the researcher for purposes of creating the de-identified data set (even if the researcher is the intended recipient of the de-identified data set). Additional information regarding "Business Associate" requirements is set forth in section iii "Business Associates" under HIPAA below.

(c) Limited Data Sets

Certain research projects require use of data (PHI) that does not meet the Privacy Rule's standards for de-identification. For such cases, the Privacy Rule permits a Covered Entity to release a "Limited Data Set." In a Limited Data Set, direct identifiers have been removed but certain potential identifiers remain. Unlike de-identified data, a Limited Data Set may include five-digit zip codes, other geographic subdivisions (such as state, county, city), and elements of date. These geographic designations are permitted in order to support a range of research and public health activities, such as the analysis of local variations in disease burdens or statistics on the provision of health care services.

To qualify as a Limited Data Set, the following direct identifiers of the individual or of relatives, employers, or household members of the individual must be removed:

1. Names.
2. Postal address information, other than town or city, state, and ZIP Code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers.
8. Health plan beneficiary numbers.
9. Account numbers.
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints and voiceprints.
16. Full-face photographic images and any comparable images.

A Limited Data Set is still considered to be PHI under HIPAA. Prior to disclosing the Limited Data Set, the Covered Entity releasing the Limited Data Set and the researcher's institution must execute a Data Use Agreement. The agreement must contain the following elements:

1. The permitted uses and disclosures by the recipient;
2. The approved users and recipients of the data;

3. Agreement by the recipient not to re-identify the data or contact the individuals;
4. Assurances that the recipient will use appropriate safeguards to prevent use or disclosure of the Limited Data Set other than as permitted by the Data Use Agreement;
5. Agreement that the researcher will report to the Covered Entity any uses or disclosures of the Limited Data Set which were not specifically allowed; and
6. Agreement to require that any agents and subcontractors adhere to the same safeguards.

The proposed Data Use Agreement must be submitted with the HSCL application. A sample Data Use Agreement can be found on the [HSCL & HIPAA Forms page](#).

As in the case of de-identified data, in order for a researcher to view a Covered Entity's records containing PHI and from those records extract a Limited Data Set, one of the Privacy Rule's conditions for disclosure of the PHI to the researcher must be met. However, a Covered Entity may provide PHI, including direct identifiers, to a "Business Associate" for purposes of creating a Limited Data Set (even if the Business Associate is the intended recipient of the Limited Data Set). Additional information regarding Business Associate requirements is set forth in section iii "Business Associates" under HIPAA below.

(d) Reviews that are Preparatory to Research

A separate exception to HIPAA's individual authorization requirement permits a researcher to access PHI from a Covered Entity if the researcher attests in writing that:

- The information is being sought solely to prepare a research protocol or for similar purposes preparatory to research;
- No PHI is to be removed from the Covered Entity by the researcher; and
- The information being sought is necessary for research purposes.

A sample request form, which includes these written attestations, can be found on the [HSCL & HIPAA Forms page](#).

This exception to the written authorization requirement may be useful for examining medical records in order to formulate hypotheses, assess feasibility of a project, or determine availability of data. However, HIPAA requires that any information recorded in that review must meet the de-identification standards set forth in section ii(b) De-identification above. As a result, researchers may not remove data such as the subject's name and contact information from the Covered Entity's premises.

(e) Waiver of Individual Authorization

Some research projects do not require written consent from the research subject. HSCL may approve a waiver of written consent if the risk is minimal, informed consent is not practicable, and a waiver of consent does not adversely affect the rights of the subject. For these studies the researcher may apply also for a waiver of the privacy Authorization requirements under HIPAA if the research meets the following criteria:

- 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;
 - 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 conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
 - 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 study, or for other research for which the use or disclosure of PHI would be permitted by HIPAA;
- The research could not practicably be conducted without the alteration or waiver; and
- The research could not practicably be conducted without access to and use of the PHI.

The researcher must apply for the Waiver of Authorization located on the [HSCL & HIPAA Forms](#) page. If the waiver is approved, the researcher must submit the form indicating such approval to the Covered Entity holding the PHI, for example the hospital holding the medical records, prior to receiving the PHI.

Studies that are exempt under HSCL standards may require a HIPAA waiver if the researcher must access PHI to perform the data collection. However, if the Covered Entity performs the data extraction and delivers only de-identified information to the researcher, no HIPAA waiver is required. Retrospective medical chart reviews generally will require a waiver of the privacy authorization since the researcher has access to the fully identifiable medical record.

(f) Research on Decedents

In order to access medical records of decedents, HIPAA requires a researcher to provide a Covered Entity with representations that the information is being sought solely for research on decedents, and that it is necessary for research purposes. The Covered Entity has a right to require documentation of the death of the individual(s). A sample PHI request form, which includes the representations described above, can be found on the [HSCL & HIPAA Forms](#) page.

(g) Related Issues

1. Notifying Research Subjects of Their Privacy Rights

Since April 14, 2003, HIPAA's Privacy Rule has required covered health care providers to provide their patients with a Notice of Privacy Practices (NPP). The NPP describes the privacy practices of the Covered Entity and informs the patients of their privacy rights with respect to their personal health information.

For certain studies involving Covered Entities and clinical interventions, contact with a researcher may be the first occasion at which the NPP is provided to an individual. Therefore, researchers involved in this type of research must check with their department/unit to determine whether they are subject to the NPP distribution requirements. If so, delivery of the NPP should accompany the signing of the privacy authorization and the acknowledgement of the receipt of the NPP must be retained. Questions regarding this requirement may be addressed to the Covered Entity involved or The Privacy Office, Lawrence Campus, 864-9528.

2. Research Recruitment under HIPAA

Health care professionals involved in the treatment of patients are allowed to discuss with their patients the option of enrolling in a research study without obtaining prior authorization from the patient. For example, a healthcare provider could give a patient a researcher's contact information so that the patient could initiate contact with the researcher. However, some form of HIPAA compliant privacy permission (e.g. a written authorization or waiver of the authorization) may be required if the healthcare provider would like to share PHI with a researcher for recruitment purposes.

An outside researcher cannot rely on the exception to the authorization requirement for reviews that are "preparatory to research" to access and use a Covered Entity's PHI to contact prospective research subjects. A properly written authorization form, or waiver for recruitment purposes, would allow the researcher to view patients' PHI in order to make determinations about study eligibility. Once a potential research subject has been identified, the researcher should follow appropriate ethical standards about contacting the patient. The initial contact should come from someone whom the patient knows has legitimate knowledge of his or her health status. The researcher will also need to make sure that appropriate authorization exists to cover use and disclosure of any PHI collected from participants identified in the recruitment process.

3. Research Repositories

HIPAA specifies three ways in which PHI held by a Covered Entity can be compiled for a research data repository:

- Individual, written Authorization is obtained from the subject of the information;
- Waiver of the individual Authorization requirement is obtained from an IRB or Privacy Board; or
- The PHI is obtained from a Covered Entity in a Limited Data Set and accompanied by a Data Use Agreement.

Future disclosures of the data in the repository must comply with applicable laws, including HIPAA. To the extent the data is held by a Covered Entity, future disclosures would be permitted if covered by an individual authorization, pursuant to an IRB waiver, or as a Limited Data Set (with a Data Use Agreement).

4. "Minimum Necessary" Standard and Role-Based Access

When conducting research involving the use or disclosure of PHI, the researcher should request from the Covered Entity only the minimum necessary PHI to accomplish the research purpose. For example, access to an entire medical record should not be requested if a portion of the records, e.g., those generated during a limited time period, would be sufficient. The Covered Entity's disclosure of the PHI to the researcher may reasonably rely on the researcher's representation that the information requested is indeed the minimum necessary.

University researchers are responsible for designating the personnel who need access to study files that contain identifiable data. Access must be commensurate with the personnel's role on the research project. Access must be limited to the minimum level of PHI appropriate to the personnel's job function.

5. Transition Requirements for Ongoing Research

The Privacy Rule includes a limited provision that "grandfathers" in certain permissions obtained for research that were acquired prior to the compliance date (April 14, 2003). Under these provisions, a Covered Entity may use and disclose PHI for the research purposes allowed by those permissions that were created or received, either before or after the compliance date, if any one of the following was obtained before the compliance date:

- An Authorization or other express legal permission from an individual to use or disclose PHI for the research.
- The informed consent of the individual to participate in the research.
- The waiver of informed consent by an IRB.

However, if a waiver of informed consent was obtained prior the compliance date, but informed consent is sought from the research subject after the compliance date, the Covered Entity must obtain the individual's Authorization as required under the Privacy Rule, unless such use or disclosure is permitted without Authorization.

The Privacy Rule allows Covered Entities to rely on express legal permission, informed consent, or IRB-approved waiver of informed consent obtained before the compliance date to use and disclose PHI for research studies, as well as for any future research that may be included in such permission. This provision is different from those applying to an Authorization or waiver obtained after the compliance date. Authorizations and waivers after the compliance date will only permit the use and disclosure of PHI for the specific research study for which they were obtained.

In some instances, existing express legal permissions, informed consents, or IRB-approved waivers of informed consent are not study specific. These permissions for research and waivers, even if provided for future unspecified research, are grandfathered in by the transition provisions, provided the permission or waiver was obtained prior to the compliance date and informed consent for research is not sought later.

6. Accounting for Research Disclosures

Under HIPAA, Covered Entities are required to provide patients (on request) with an accounting of certain disclosures of the patient's PHI. Disclosures made by a Covered Entity under a waiver of Authorization, for activities preparatory to research or for studies on decedents, must be tracked in the medical record and accounted for if requested. Among the types of disclosures that are exempt from this accounting requirement are research disclosures made pursuant to an individual's Authorization and disclosures of the Limited Data Set to researchers with a Data Use Agreement.

Researchers involved in clinical trials that involve the delivery of routine health care, such as an MRI or liver function test, may be subject to this requirement. For additional information regarding these requirements, contact The Privacy Office, Lawrence Campus, at 864-9528.

iii) "Business Associates" under HIPAA

In addition to permitting a Covered Entity to disclose PHI to a researcher if certain conditions are met, the Privacy Rule allows a Covered Entity to disclose PHI to a "Business Associate" helping

the Covered Entity to carry out its health care activities. The Privacy Rule includes separate requirements regarding such disclosures. The Covered Entity must obtain satisfactory written assurances about how the Business Associate will handle the PHI it receives or collects on behalf of the Covered Entity. These written assurances are usually called a "Business Associate Agreement." They may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate Business Associate Agreement. It is also permissible for a Business Associate Agreement to refer to an underlying services agreement when specifying permitted uses and disclosures.

A Business Associate Agreement **is not** required if the Covered Entity has determined that the Business Associate will be accessing and handling only "De-identified" data (see section iii "Business Associates" under HIPAA) or if all disclosures to the Business Associate are covered by individual Authorizations which meet HIPAA's Authorization requirements.

Business Associate Agreements must be in the format approved by the university for this purpose, and they must be approved and executed in accordance with university contracting policies. Questions regarding Business Associate Agreements, or requests for approval of such an agreement, may be addressed to Contract Negotiations and Research Compliance at 864-7431 or, if not part of a sponsored project, to The Privacy Office, at 864-9528 or University General Counsel.

a) Who May Qualify as a Business Associate?

A Business Associate Agreement is required when a person or entity outside a Covered Entity receives PHI from the Covered Entity in the course of conducting a "covered" activity on behalf of the Covered Entity. The Privacy Rule lists some of the activities and services that make a person or entity a Business Associate, if the activity or service involves the use or disclosure of PHI.

Business Associate activities include:

- claims processing or administration;
- data analysis, processing or administration;
- utilization review;
- quality assurance;
- billing;
- benefit management;
- practice management;
- repricing.

Business Associate services include:

- legal;
- actuarial;
- accounting;
- consulting;
- data aggregation;
- management;
- administrative;
- accreditation;

- financial.

As stated in section ii Personal Health Information and Research under HIPAA above, an activity is generally considered to be research if it is intended to contribute to "generalizable knowledge." Research is not a "covered" activity under HIPAA, and researchers who legitimately receive PHI from a Covered Entity by meeting one of the conditions outlined in section ii do not need a Business Associate Agreement, even if the Covered Entity has hired the researcher to perform research on the Covered Entity's behalf. Likewise, a Business Associate Agreement does not grant the right to conduct research involving PHI, since research is not a "covered" function. A Covered Entity is only permitted to disclose PHI for research purposes as permitted by the Privacy Rule; that is, if the requirements described in section ii are met. In some cases, it may be difficult to distinguish whether an activity is "research" or a "Business Associate" service. In other cases, both types of activities may be occurring at the same time.

Following are some examples of Business Associates and non-Business Associates:

Example 1: X is contracted by a Covered Entity (a state Medicaid agency) to assist the Covered Entity in conducting an internal evaluation of its enrollment operations. In the course of providing these services, X will be provided with individually identifiable health information regarding certain Medicaid beneficiaries. X is likely a Business Associate of the Covered Entity.

Example 2: Same as Example 1, however, the information disclosed to X in the course of providing the services will be "de-identified" as defined by HIPAA. No Business Associate Agreement is needed because the information is "de-identified."

Example 3: Same as Example 1, however, X would like to be able to use the PHI for her department's own research purposes. The Covered Entity agrees. X is both a Business Associate and a researcher. The Covered Entity is not permitted to allow a Business Associate to use the PHI for research purposes unless the Privacy Rule's research requirements are met. Since obtaining written Authorization from the Medicaid beneficiaries is not practicable, an exception to the research Authorization requirements will have to be met. For example, X could discuss with the Covered Entity the possibility of the Covered Entity stripping the data of identifiers prior to X's using it for the separate research purposes. Or, it might be possible for X to assist the Covered Entity in stripping the data to prepare a "de-identified" or "limited data set" as permitted by HIPAA (see section iii(b) Use of Data by a Business Associate for Separate Research Purposes below), if the activity is covered by a Business Associate Agreement. In the case of a "limited data set," X would also have to sign a "Data Use Agreement" to cover the research use of the data.

b) Use of Data by a Business Associate for Separate Research Purposes

KU Researchers serving as Business Associates may likely be interested in using a Covered Entity's data for research (as opposed to using it only to carry out the Business Associate services). It must be remembered that the rules regarding a Covered Entity's disclosure of PHI to a Business Associate for Business Associate purposes are different from the rules regarding a Covered Entity's disclosure of PHI to a researcher for research purposes. For this reason, it is important to clarify the various types of activities that may occur **and to document those activities specifically in any agreements between KU/KUCR and the external agency.** Moreover, care must be taken to ensure that requirements specific to a Business Associate relationship (such as requirements regarding individuals' access to their PHI or requirements

regarding return of PHI to a Covered Entity) are not inappropriately imposed in a research context.

1) De-identified Data

Covered Entities may use or disclose health information that is "de-identified" without restriction under the Privacy Rule and no Business Associate Agreement or individual authorization is required (see section ii(b) De-identification above regarding de-identification of data). In some cases, it may be impractical for the Covered Entity to de-identify the data. According to the U.S. Department of Health and Human Services, Covered Entities may permit a Business Associate to de-identify its data for research purposes, even if the Business Associate is the intended recipient of the data set. A Business Associate Agreement permitting de-identification of the data is required. The data recipient, as a Business Associate, must agree to return or destroy the information that includes the direct identifiers once it has completed the conversion of the data.

2) The Limited Data Set Alternative

It is also possible for a Covered Entity to enter into a Business Associate Agreement with a researcher to create a Limited Data Set for research purposes. A Business Associate Agreement permitting creation of the Limited Data Set by the researcher is required and the researcher, in his/her role as a Business Associate, must agree to return or destroy the information that includes the direct identifiers once it has completed the conversion of the data. Because the Privacy Rule conditions disclosure of a Limited Data Set on the Covered Entity's obtaining a "Data Use Agreement" from the data recipient, the Business Associate would also have to enter into a Data Use Agreement with the Covered Entity (see section ii(c) Limited Data Sets above). The provisions of the Data Use Agreement may be incorporated into a Business Associate Agreement.

c) Standard Business Associate Agreement Provisions: What They Require

1. Do not use or disclose PHI except as provided for in the Business Associate Agreement:

Business Associate Agreements are required to set forth the permitted and required uses of PHI by the Business Associate. For this reason, the parties must communicate clearly about the uses and disclosures that will be necessary to provide services to the Covered Entity. The Business Associate Agreement will state that the Business Associate will not use or further disclose the PHI other than as permitted or required by the agreement or as required by law. **It cannot authorize the Business Associate to use or further disclose the PHI in a manner that would violate the requirements of HIPAA if disclosed by the Covered Entity.** All persons working on a project subject to a Business Associate Agreement must understand the uses and disclosures permitted by the Business Associate Agreement and must comply with all restrictions.

2. Use appropriate safeguards to protect the PHI:

Business Associate Agreements require the Business Associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the Business Associate Agreement. What constitutes "appropriate safeguards" will vary depending on the nature and circumstances of the project involved. Attention must be paid to administrative safeguards (such as written policies and procedures), physical safeguards (such as ensuring paper files containing PHI are locked) and technical safeguards (such as ensuring that electronic PHI is stored in a secure manner). Additional information regarding appropriate safeguards can be obtained by contacting The Privacy Office, Lawrence Campus at (785) 864-9528.

3. Report unauthorized disclosures to the Covered Entity:

Business Associate Agreements require a Business Associate to report unauthorized disclosures of the PHI to the Covered Entity. Reports to the Covered Entity must be made in the manner outlined in the Business Associate Agreement. Therefore, in the event of an unauthorized disclosure, the terms of the Business Associate Agreement, in addition to university policies regarding reporting and handling of violations, must be considered.

It should be noted that when a Covered Entity knows of a material breach or violation by the Business Associate, the Covered Entity is required to take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, to terminate the agreement or arrangement. If termination of the agreement is not feasible, a Covered Entity is required to report the problem to the Department of Health and Human Services (DHHS) Office for Civil Rights (OCR).

4. Require subcontractors and agents to agree to comply:

If the Business Associate provides the PHI to any subcontractors working on the project, the Business Associate must obtain the subcontractor's agreement to abide by the same restrictions and conditions that apply to the Business Associate with respect to the PHI. This agreement must be in writing in the form approved by the university for this purpose. An agreement for subcontractors or agents participating in an externally sponsored project may be obtained by contacting Contract Negotiations at (785) 864-7431 or, if not part of a sponsored project, The Privacy Office, at (785) 864-9528.

5. Make PHI available to individuals to access or amend their PHI or to receive an accounting of disclosures:

Covered Entities are required to provide the individuals to whom the PHI pertains the opportunity to access and amend their own PHI. Because of these requirements, the Covered Entity must specify in the Business Associate Agreement that the Business Associate will make PHI available to the Covered Entity if and when it is needed by the Covered Entity to comply with its access and amendment obligations. While the Covered Entity itself is responsible for addressing requests from individuals regarding these rights, the Business Associate Agreement may ask the Business Associate to receive and address individuals' requests on behalf of the Covered Entity.

It is important to note that the right to access, copy, or amend PHI applies only to PHI included in the Covered Entity's "Designated Record Set" (DRS). A DRS consists of those records maintained by or for a Covered Entity. For example, 1) for a provider, such records could include the medical records and billing records about the individuals; 2) for a health plan, they could include the enrollment, payment, claims adjudication and case or medical management record systems; or 3) for any Covered Entity they could include any personally identifiable information used in whole or in part by or for the Covered Entity to make decisions about individuals. The DRS may include the above types of records when in the possession of a Business Associate, **unless the information held by the Business Associate merely duplicates the information maintained by the Covered Entity.** For this reason, it is important to clarify "up front" whether the PHI accessed, received or created by the Business Associate on behalf of the Covered Entity is considered part of the Covered Entity's DRS. If the PHI is subject to these access and amendment rights, the project involved must have in place systems to support them.

Similarly, individuals to whom PHI pertains have the right to request an "accounting" or list of certain disclosures that have been made by the Covered Entity (or Business Associates working on the Covered Entity's behalf). This requires the Covered Entity (or the Business Associate working on the Covered Entity's behalf) to document on an ongoing basis when certain types of

disclosures are made. Because of this requirement, the Covered Entity will likely specify in the Business Associate Agreement that the Business Associate will make information about certain disclosures available to the Covered Entity if and when it is needed by the Covered Entity to comply with its accounting obligations. In some cases, the Business Associate Agreement may ask the Business Associate to receive and address individuals' requests on behalf of the Covered Entity. There are a number of exceptions to the accounting requirement, many of which could apply to certain projects carried out by the university for outside Covered Entities. For example, accounting is not required for disclosures to the individuals to whom the PHI pertains or their legal representatives. Nor is it required for disclosures made pursuant to a written Authorization from the individual. Nevertheless, it is important to clarify "up front" whether systems to support these accounting requirements will need to be put in place.

6. Make internal records available to DHHS for compliance:

A Business Associate is required to make available to the Secretary of the U.S. Department of Health and Human Services internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received on behalf of the Covered Entity for purposes of determining the Covered Entity's compliance with HIPAA. In the event of a request for information by DHHS, the Office of the General Counsel at the University of Kansas should be contacted immediately for assistance.

7. Return or destroy PHI upon termination of Business Associate Agreement:

When a Business Associate Agreement terminates, the Business Associate is required to return or destroy all PHI received from, or created/received on behalf of the Covered Entity, if feasible.

Copies may not be retained. If return is not feasible, and the information must be retained for specific reasons and uses, such as for future audits, the Covered Entity must be notified in the manner set forth in the Business Associate Agreement. In such cases, the protections of the Agreement must be extended to the PHI for as long as the PHI is retained, and further use and disclosure must be limited to those purposes that make the return or destruction infeasible.

8. Provide Access to Covered Entity for Purposes of Assessing Compliance: Some Covered Entities may require that the Business Associate make project-related records available for purposes of determining compliance with privacy laws and the Business Associate Agreement. Similarly, some Covered Entities may request copies of the Business Associate's policies and procedures as they relate to the handling of PHI received from, created, or received on behalf of the Covered Entity.

d) Steps to Take as a Project Director

It is important to develop a plan for ensuring the privacy and security of PHI accessed or obtained in the course of providing services to a Covered Entity. Developing an appropriate plan includes, but is not limited to, the following:

- Designate a person to coordinate privacy and security issues on the project.
- Assess PHI flow, uses and disclosures so that there is a clear picture of where PHI will travel and the uses and disclosures that will need to be made.
 - Uses and disclosures must comply with the Business Associate Agreement (and applicable laws).
 - Uses and disclosures not permitted by the Business Associate Agreement must be pre-approved (in writing) by the Covered Entity (this includes the use of PHI for research and educational purposes).

- Only the "minimum necessary" PHI should be provided by the Covered Entity.
- Treat persons not on the project team as you would "outside entities," even if they are also employed by the university. In other words, DO NOT disclose the PHI to them unless the disclosure is permitted or required by law.
- Develop the policies and procedures needed to provide persons working on the project with guidance on the appropriate handling, use or disclosure of the PHI.
- Determine what steps (technical and non-technical) will be needed to ensure that the PHI is protected from unauthorized uses and disclosures.
- If PHI in your possession is subject to the individuals' rights to access, amendment or accounting, develop the processes needed to respond to requests from the Covered Entity (or the individual).
- Educate all persons working on the project (including students) about the permitted uses and disclosures, procedures to safeguard privacy and security, and their obligations to comply with the terms of the Business Associate Agreement. Document this education by means of a training log or other appropriate means.

Much of the information contained in this section has been taken from materials published by the U.S. Department of Health and Human Services, including the booklet, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*. Additional information regarding HIPAA's Privacy and Security Rules may be obtained at the [US Department of Health & Human Services HIPAA web page](#). Questions regarding HIPAA or the applicability of other state and federal laws may be addressed to:

- Contract Negotiations at (785) 864-7431
- David Hann, Coordinator, Human Subjects Committee, Lawrence Campus at (785) 864-7429 or dhann@ku.edu.
- The Privacy Office, Lawrence Campus, at (785) 864-9528.

iv) HIPAA-Related Forms and Templates

All HIPAA-related forms and templates can be found on the [Human Subjects Committee - Lawrence Campus \(HSCL\) & HIPAA Forms page](#).