

**YALE UNIVERSITY**  
**THE RESEARCHERS' GUIDE TO HIPAA PRIVACY**

**Health Insurance Portability and Accountability Act of 1996**

**Handbook**

**Table of Contents**

**I. Introduction**

- What is HIPAA?
- What is PHI?
- What is a covered entity?
- What research activities are covered by HIPAA?

**II. HIPAA's Impact On Research Protocols**

- Requirements for Research Use of PHI
- Research Using or Creating PHI of Living Individuals
- Consent Obtained Prior to April 14, 2003
- Research Under a Participant's Authorization
- Waiver of Authorization
- Activities Preparatory to Research
- Research on Decedents
- Recruitment
- De-identified Data
- Limited Data Sets & Data Use Agreements
- Databanks and Repositories
- Studies Exempted from IRB Review
- International Research
- Resignations of Investigators or Research Staff

**III. Patient's Rights Provisions in Research Studies**

- Notice of Privacy Practices
- Individual Right to Access and Amendment
- Accounting for Disclosures
- Record Retention

**IV. Privacy and Security Measures**

**V. Resources and Links**

**VI. Researcher Certification**

## I. INTRODUCTION

### **What is HIPAA?**

HIPAA is the Health Insurance Portability and Accountability Act of 1996. HIPAA requires many things, including the standardization of electronic patient health, administrative and financial data. It also establishes security and privacy standards for the use and disclosure of “protected health information” (PHI).

The HIPAA Privacy Rule:

- Establishes conditions under which PHI can be used within an institution and disclosed to others outside it;
- Grants individuals certain rights regarding their PHI;
- Requires that institutions maintain the privacy and security of PHI.

This guide addresses HIPAA’s requirements related to uses and disclosures of PHI for research purposes. It does not cover HIPAA’s requirements related to uses and disclosures of PHI for other purposes (such as treatment, payment, or health care operations). If you need guidance on these issues, please refer to <http://hipaa.yale.edu/>.

### **What is PHI?**

HIPAA’s regulatory provisions apply to the use and disclosure of protected health information (PHI). PHI is defined as individually identifiable health information that is created or received by a HIPAA “covered entity” (see definition below).

Health information includes any information, whether oral or recorded in any form, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for health care to an individual.

## Researchers' Guide to HIPAA Privacy

PHI is considered individually identifiable if it includes **one or more** of the following identifiers:

1. Names
2. All geographic subdivisions smaller than a State, including:
  - street address
  - city
  - county
  - precinct
  - zip codes and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly-available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. Telephone numbers
4. Fax numbers
5. E-mail addresses
6. Social Security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. All elements of dates (except year) for dates related to an individual, including:
  - birth date
  - admission date
  - discharge date
  - date of death
  - 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
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying numbers, characteristics, or codes

### **What is a covered entity?**

HIPAA applies to “covered entities,” which are defined as health plans, health care clearinghouses, and health care providers that transmit health information related to insurance coverage electronically. At Yale, such transactions occur in the School of Medicine (YSM), School of Nursing (YSN), University Health Services (UHS), and the Department of Psychology Clinics. These units of the University are considered to be part of the Yale University covered entity. Other segments of the University, such as the Faculty of Arts and Sciences, are not subject to HIPAA. Although not all of YSM and YSN are involved in the requisite electronic transactions, they have been included as a whole within the covered entity. This decision was based on an analysis of the projected impact of HIPAA’s administrative requirements related to transfer of information out of the covered entity and the concomitant barriers to communication inherent in further subdividing YSM and YSN under HIPAA.

### **What research activities are covered by HIPAA?**

At Yale, research activities involve PHI and thus are subject to HIPAA if all of the following conditions are met:

- The data includes any of the identifiers listed above, AND
- The data includes health information, AND

## Researchers' Guide to HIPAA Privacy

- The data is created or received by YSM, YSN, YUHS, the Psychology Clinics or any other covered entity.

Yale has developed procedures to assist researchers in determining which research activities involve PHI. These procedures can be found at <http://info.med.yale.edu/hic/>.

## II. HIPAA'S IMPACT ON RESEARCH PROTOCOLS

HIPAA's requirements relating to research do not replace or eliminate the requirements of the federal Common Rule. All Common Rule requirements (e.g., IRB approval of human subjects research) still apply.

HIPAA does add certain new requirements to research. Under HIPAA, the use or disclosure of PHI for research purposes requires a signed Research Authorization Form from the research subject unless an exception under HIPAA applies. HIPAA also applies to certain research related activities that are not covered under the Common Rule, e.g., research on decedents or studies determined to be exempt from IRB review.

In addition, HIPAA introduces a concept known as the "minimum necessary" standard. In general, HIPAA requires that only the minimum necessary PHI should be used unless the PHI is used for treatment, or unless the use or disclosure is made subject to a written authorization (including a research authorization). Thus, the minimum necessary standard requires researchers who are engaging in research, but do not have a HIPAA research authorization, to limit their access of PHI to only that needed to accomplish the research initiative and the intended purpose of the use and/or disclosure of PHI.

The additional requirements mandated by HIPAA, as they relate to research access to PHI, are described below.

### **Requirements for Research Use of PHI**

The Privacy Rule applies to the following types of research activities when they involve PHI:

- Research using or creating PHI about living individuals
- Activities preparatory to research
- Research on decedents
- Recruitment
- Research using a Limited Data Set
- Collection of PHI of secondary subjects

The types of research that do not fall under the HIPAA Privacy Rule are:

- Research using de-identified data, i.e., data that contains none of the 18 HIPAA identifiers
- Research conducted by an individual who is not part of a HIPAA covered entity and that does not require access to information held by a HIPAA covered entity

## Researchers' Guide to HIPAA Privacy

Yale has developed a form to facilitate compliance with HIPAA and access to PHI by outlining the required documentation or certifications that researchers must use in order to access PHI. Researchers should complete the "Request for Access to PHI for Research Purposes" form and provide it and the supporting documentation (described on the form) to the entity responsible for the PHI of interest. Both Yale University and Yale-New Haven Hospital (YNHH) have approved the use of this form. Note that the form does not describe the requirements for access to a Limited Data Set. Access to a Limited Data Set requires a more detailed agreement as described below.

### **Research Using or Creating PHI of Living Individuals**

PHI may not be used for research purposes unless at least one of the following applies:

- The researcher has informed consent documents or waivers of informed consent obtained prior to April 14, 2003
- The researcher obtains subjects' HIPAA authorization for the research
- The IRB approves a waiver of HIPAA authorization for the research
- The study involves only de-identified data or a Limited Data Set

### **Consent Obtained Prior to April 14, 2003**

Researchers may continue to use or disclose PHI obtained or created before April 14, 2003 pursuant to the informed consent document for that research study. A Research Authorization Form or request for a waiver is not required if the subjects signed informed consent forms to participate in the research prior to April 14, 2003. Contact with research participants and data collection may continue without a HIPAA Research Authorization Form based on the existence of an informed consent form signed prior to April 14, 2003.

Alternatively, researchers may continue to use or disclose PHI in studies for which there is an approved IRB Waiver of Informed Consent under 45 CFR 46.116(d).

If it becomes necessary to re-consent any participants in such studies after April 14, 2003, researchers must obtain a HIPAA compliant Research Authorization Form or an approved request for waiver of HIPAA authorization in order to obtain or create PHI.

### **Research under a Participant's Authorization**

As mentioned above, HIPAA generally requires a written authorization from the subject permitting a researcher to use or disclose the subject's PHI for research purposes. The researcher is required to obtain written authorization from the research participants via a signed [Research Authorization Form](#). For an incompetent adult subject or a minor subject, a Personal Representative, someone with the legal authority to act on behalf of the subject, should sign the form exercising the subject's rights related to the individual's protected health information. The written Research Authorization Form must contain:

- A specific description of the PHI that will be used and/or disclosed.
- The names of persons or organizations that may use or disclose the PHI.

## Researchers' Guide to HIPAA Privacy

- The names of persons or organizations to whom the PHI will be disclosed.
- A statement of the purpose of the use and/or disclosure.
- A statement of how long the use and/or disclosure will continue (no expiration date is permitted for research purposes, however this must be specifically stated in the authorization form and justification must be provided in the protocol).
- A statement that the subject can revoke his or her authorization.
- A statement regarding the potential for re-disclosure to others not subject to the HIPAA Privacy Rule.
- A notice that the covered entity either may or may not condition treatment or payment on the individual's signature.
- The individual's signature and the date.

Permissible uses and disclosures are limited to those described in the [Research Authorization Form](#). If a researcher needs to disclose PHI to a person or organization not listed in the Research Authorization Form, the researcher should obtain an additional written Research Authorization from the subject or apply to the IRB for a waiver of Authorization.

The [Yale University Research Authorization Form](#) provides standard language for the required statements listed above. Investigators using this form need only specify to whom and where PHI will be sent and what type of PHI will be disclosed. Authorization forms not based on the Yale template or that modify or remove language from the template are subject to review by the Privacy Office. Research Authorization Forms will generally be separate from the Informed Consent Documents but signed at the same time.

Disclosures of PHI made in connection with research conducted pursuant to signed authorization do not need to be tracked for purposes of responding to an individual who requests an accounting of disclosures (see *Accounting for Disclosures* below).

Research Authorization Forms will usually become part of the individual's medical record. The use of a compound Authorization (e.g., informed consent document plus Research Authorization Form combined) is not appropriate in cases where the compound Authorization will become part of the medical record. The informed consent document usually contains additional information (i.e., information in addition to that required by HIPAA for the Research Authorization Form), and this additional information may not be appropriate for inclusion in the permanent medical record.

Investigators should include completed Research Authorization Forms with the protocol package and submit it to the IRB for expedited review. Investigators will receive from the IRB a stamped Research Authorization Form, which acknowledges IRB receipt and acknowledges that the form will be used in the research protocol.

Copies of the signed Research Authorization Form and the [Request Access to PHI for Research Purposes](#) form should be provided to the record holder to obtain access to the appropriate records.

### **Waiver of Authorization**

## Researchers' Guide to HIPAA Privacy

If the research study involves PHI and certain other conditions exist, the researcher may request, and the IRB may grant, a [waiver of HIPAA authorization](#).

A waiver of HIPAA authorization is permitted only when all of the following exist :

- The research could not be practicably conducted without the waiver.
- The research could not be practicably conducted without access to and use of PHI.
- The researcher provides written assurance to the IRB that the PHI will not be re-used or disclosed (except as required by law, or for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by the HIPAA Privacy Rule).
- The use(s) and/or disclosure(s) of PHI will be limited to the minimum necessary standard.
- The use(s) and/or disclosure(s) involve no more than minimal privacy risk to the subjects.
- The IRB has reviewed and approved the proposed use(s) and disclosure(s) of PHI.

Researchers can request a waiver of Research Authorization by completing the [Yale University Request for HIPAA Waiver of Authorization for Research Form](#) and submitting to the IRB for review and approval. The following must be clearly articulated in the waiver application:

- Why the research could not practicably be conducted without the waiver.
- Why the research could not practicably be conducted without access to and use of the PHI.
- A written assurance to the IRB that the PHI will not be re-used or disclosed except as required by law, for authorized oversight of the research, or for other research.
- A written statement describing the PHI that will be used and/or disclosed and an explanation of how the use(s) and/or disclosure(s) of PHI will meet the “minimum necessary” standard.
- A statement that the use(s) and/or disclosure(s) involve no more than minimal privacy risk to the subjects.
- A description of the plan to protect identifiers.
- A description of the plan to destroy the identifiers as quickly as possible.
- A description of the plan to track disclosures.

The criteria for waiver of Research Authorizations are similar to those for waiving informed consent. Therefore, if the research plan includes obtaining informed consent from research participants, it is unlikely that the IRB will approve a waiver of a HIPAA Research Authorization, except perhaps for recruitment purposes (*see Recruitment Section*). Disclosures of PHI that are made in connection with research conducted pursuant to a Waiver of HIPAA Authorization must be tracked in order to respond to individuals who request an accounting of disclosures of their PHI. Investigators are responsible for tracking such disclosures made in connection with their own research protocols. (*See Yale's policy on accounting for disclosure at <http://www.yale.edu/ppdev/policy/5003/5003.html>*)

Investigators should include the completed [Yale University Request for HIPAA Waiver of Authorization for Research Form](#) with the protocol package and submit it to the IRB.

## Researchers' Guide to HIPAA Privacy

In most cases, the IRB will assess the request using an expedited review process. However, full IRB committee review is required in cases in which a waiver has been requested by the investigator, but risk to the individual's privacy is greater than minimal. Investigators will receive from the IRB an authorized Approval/Denial of Waiver of HIPAA Authorization.

Copies of the waiver of Research Authorization and the [Request Access to PHI for Research Purposes](#) form should be provided to the record holder to obtain access to the appropriate records.

### **Activities Preparatory to Research**

Investigators may access PHI in activities that are "preparatory to research." This type of access is limited to a review of data to assist in formulating a hypothesis, determining the feasibility of conducting the study, determining cell size, or other similar uses that precede the development of an actual protocol.

While an investigator may review PHI during the course of a review preparatory to research, he or she may not remove, copy, or include any PHI in notes. Investigators may not use PHI to identify potential research subjects by name or by any other HIPAA identifier. However, investigators may write down and remove summary data (e.g., number of individuals with a certain disease).

Before accessing PHI for a review preparatory to research, a researcher must provide written assurances to the holder of the PHI that the review of the PHI is necessary to prepare a research protocol and that the PHI will not be removed by the researcher from the entity. No further review or approval is required.

Researchers wishing to conduct activities preparatory to research using Yale University or Yale-New Haven Hospital medical records must complete the [Yale-New Haven Health Systems/Yale University Request for Access to Protected Health Information for a Research Purpose](#). Clinical administrators are not permitted to run IDX reports for research purposes. Researchers should forward all requests for IDX reports to the Yale Medical Group using the appropriate form.

### **Research on Decedents**

HIPAA requires that researchers who wish to access PHI of decedents for research purposes first make certain written representations to the holder of the PHI. The researcher must first represent that the use or disclosure of PHI is solely for research on the PHI of decedents. That is, the researcher may not use the PHI of the decedent to obtain information about a decedent's living relative(s). A researcher *may* request a decedent's medical history for an outcome study relating to treatment previously administered to the decedent. The researcher must also provide written assurance that the PHI is necessary for the research. The holder of the PHI has a right to require documentation of death of the individuals about whom information is sought.

## Researchers' Guide to HIPAA Privacy

Researchers wishing to conduct research on decedents using Yale University or Yale-New Haven Hospital medical records must complete the [Yale-New Haven Health Systems/Yale University Request for Access to Protected Health Information for a Research Purpose](#).

### **Recruitment**

The use of PHI to recruit an individual to participate in a research study must comply with HIPAA's general requirement that the use must be pursuant to an authorization or some exception, such as a waiver of HIPAA authorization. Although recruitment procedures usually require access to a limited amount of health information, recruitment is considered to be an accessing of PHI and, therefore, must comply with HIPAA requirements.

Treating providers may **not** disclose PHI to a third party (including a "researcher" within the same covered entity) for purposes of recruitment in a research study without first obtaining authorization from the individual.

A treating provider does, however, have the option to:

- Discuss with his/her own patients the option of enrolling in a study.
- Obtain written authorization from the patient for referral into a research study.
- Provide research information to the patient so that the patient can initiate contact with the researcher.
- Provide information to a researcher when the researcher has obtained an approved Waiver of Research Authorization from an IRB for recruitment purposes.

HIPAA also applies to recruitment and research activities conducted via medical records and medical registry reviews. Investigators must obtain either a Research Authorization from the subject or a [Waiver of HIPAA Authorization](#) approved by an IRB prior to commencing research recruitment activities from these sources. A [Waiver of HIPAA Authorization](#) for recruitment purposes only is referred to as a partial waiver. Researchers are required to obtain subjects' Research Authorizations after recruiting and enrolling subjects via a partial waiver and prior to creating or using PHI during research procedures.

Investigators should include the completed [Yale University Request for HIPAA Waiver of Authorization for Research Form](#) with the protocol package, including the [HIPAA Authorization Form](#) or Requests for Waiver of HIPAA Authorization that will be used after recruitment, and submit the protocol package to the IRB as described in the previous section on waivers.

### **De-identified Data**

De-identified data are data that contain none of the 18 HIPAA identifiers listed above in the "What is PHI?" section. If all of the 18 identifiers are removed, the information is no longer (1) individually identifiable, (2) PHI, and (3) subject to HIPAA's requirements. A de-identified data set may be coded with a unique identifier that cannot be traced back to

## Researchers' Guide to HIPAA Privacy

the individual for the purpose of being re-identified by the recipient at a later date. De-identified data may include gender, age, race, or relevant information regarding disease or tissue source and can later be re-identified, by the original holder of the data, if necessary, by means of a unique, non identifiable, code for purposes of carrying out research. It is important to remember that re-identification will subject the information to HIPAA's requirements. A researcher must resubmit the protocol to the IRB for approval when re-identification of the data is desired.

A data set may also be considered de-identified if an expert in statistical and scientific methods determines and documents that the methods used to de-identify or code the data present a very small risk that the information can be used alone or in combination with other reasonably available information to identify an individual.

“Anonymous” data are not necessarily considered de-identified under HIPAA. Anonymity under the federal Common Rule requires that individuals cannot be readily ascertained by the investigator and cannot be associated with the data. According to the Common Rule standard, anonymous data may retain dates of treatment. Under HIPAA's more stringent requirements, however, such data would be considered identifiable data.

### **Limited Data Sets and Data Use Agreements**

Some studies may need to retain a limited number of identifiers and, thus, not meet the strict HIPAA definition of “de-identified data.” However, these studies may present only minimal potential for identifying participants based on the data set. In such circumstances, HIPAA permits use of a “Limited Data Set” for research purposes. A Limited Data Set is PHI that excludes “direct identifiers” of the individual, relatives of the individual, employers, or household members.

A Limited Data Set must **exclude**:

1. Names	8. Account Numbers
2. Street Addresses	9. Certificate/Licenses Numbers
3. Phone and Fax Numbers	10. Vehicle Identifiers/License Plates
4. Email Addresses	11. Device Identifiers
5. Social Security Numbers	12. Web URLs
6. Medical Record Numbers	13. Internet Protocols (IP)
7. Health Plan Numbers	14. Full Face Photos

A Limited Data Set may include one or more of the following:

1. Towns
2. Cities
3. States
4. Zip Codes and their equivalent geocodes. (Note that a zip code cannot be used if the area composing the zip code has fewer than 20,000 citizens.)
5. Dates including birth and death
6. Other unique identifying numbers, characteristics, or codes that are not expressly excluded. (Medical record numbers and pathology numbers are excluded.)
7. Relevant medical information

## Researchers' Guide to HIPAA Privacy

A Limited Data Set may be used only for purposes of research, public health, or health care operations. It may be used only if the covered entity providing the data and the recipient of the data first enter into a [Data Use Agreement](#). The investigator, the holder of the PHI, and their respective institutions, must sign Data Use Agreements, either for access to a Limited Data Set or for the release of a Limited Data Set. At Yale, the Offices of Grant and Contract Administration will administer the negotiation and execution of these agreements. These agreements must, among other things, establish the permitted uses and disclosures of the information included in the Limited Data Set and must provide that the recipient of the Limited Data Set will not identify the information or use it to contact individuals. Yale has developed an [Internal Data Use Agreement](#) for researchers to use (1) when transferring a Limited Data Set between researchers within Yale, and (2) when bringing into Yale a Limited Data Set that has been collected by the researcher at a site not covered by HIPAA (i.e., when the data was not PHI when collected, but will become PHI when it arrives at a Yale HIPAA covered component).

As with research conducted pursuant to an authorization, disclosure(s) of PHI that are part of a Limited Data Set need not be tracked for purposes of providing an accounting to an individual.

The use of a Limited Data Set in a protocol should be specified in the research plan and confidentiality sections. The IRB will acknowledge the use of the Limited Data Set in the letter of IRB Common Rule approval sent to the principal investigator. The letter will state that the research activity cannot begin until the principal investigator has an authorized Data Use Agreement in place.

Other resources that provide information on de-identification and Limited Data Set Procedures include:

- *Yale University Policy regarding the Use and Disclosure of De-Identified Information and of Limited Data Sets at <http://hipaa.yale.edu/>*
- *Yale University Procedure on De-Identification and Limited Data Set Procedures at <http://info.med.yale.edu/hic/>*
- *The HIPAA Privacy Office*

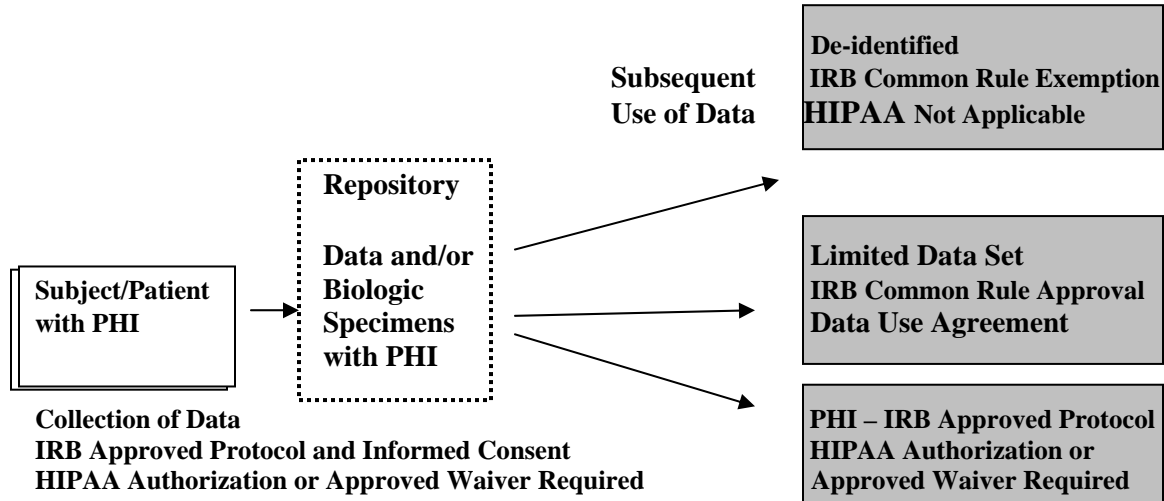
### **Databanks and Repositories**

The collection or maintenance of PHI in databanks or repositories for future research purposes requires an IRB-approved protocol. In addition, research using data from these databanks and repositories must be conducted under an IRB-approved protocol. Since databanks and tissue repositories frequently survive beyond the lifespan of the initial IRB protocol in which the data/tissue is collected, researchers should normally submit the proposed data/tissue banking activities to the IRB in a separate protocol.

The HIPAA Privacy Rule affects activities such as research using identifiable or coded data or biological specimens such as human tissue, DNA, and blood where the researcher controls the coding. The HIPAA Privacy Rule requires an authorization from the subject about whom information is stored or a HIPAA Waiver of Authorization approved by an

## Researchers' Guide to HIPAA Privacy

IRB for the collection of PHI and prior to conducting subsequent studies using PHI. The IRB must review and approve all proposed uses of stored tissues, irrespective of whether or not the secondary use(s) of the banked tissues will include use of HIPAA identifiers.



### Studies Exempted from IRB Review

Studies exempted under the Common Rule that involve the use of PHI are not exempted under HIPAA. HIPAA requirements related to authorization or waiver are applicable to these studies. Investigators should provide a Research Authorization Form or Request for Waiver of HIPAA Authorization to the IRB along with the exemption request.

### International Research and Collection of Health Information at Sites Where HIPAA Is Not Applicable

HIPAA does not apply to all sites where individually identifiable health information may be collected. For example, studies conducted at clinical facilities outside of the U.S. or health information collected from an educational record are not governed by HIPAA. Transfer of the data to a HIPAA covered component (at Yale or elsewhere), however, renders any individually identifiable health information PHI by virtue of its being held by a facility covered by HIPAA. Once the data are transferred to a HIPAA covered component, all HIPAA regulations apply.

When individual sites are not covered by HIPAA, researchers are not required to follow HIPAA's patients' rights provisions, e.g., providing a copy of the NOPP, during data collection at those sites. However, because HIPAA requirements become effective upon return of the data to a covered component at Yale, the use and disclosure of the data from Yale requires researchers to adhere to the Research Authorization requirements described above. Therefore, in these cases, when identifiable data will be brought back to a HIPAA covered component (at Yale or elsewhere), researchers should obtain HIPAA Research

Authorizations in order to reduce the need to account for subsequent disclosure(s) of the PHI. In some cases, researchers can bring the relevant data to Yale either stripped of all 18 HIPAA identifiers, with or without a code maintained at the collections site, or as a Limited Data Set with an accompanying Internal Data Use Agreement.

### **Resignations of Investigators or Research Staff**

In the event that a Yale investigator or research staff member leaves Yale and wishes to copy or remove research data created or acquired while that individual was at Yale, he or she must first request permission from his or her department chair. If the chair approves the data transfer, the request should then be submitted to the Yale HIPAA Privacy Officer. Taking data to a new institution constitutes a disclosure of PHI under HIPAA that requires tracking in the accounting for disclosures log. The Yale HIPAA Privacy Officer will make each determination related to privacy rules on a case-by-case basis, considering at a minimum the following:

- whether the data includes PHI;
- who, in addition to the departing investigator or staff member, will have access to the removed or copied data, including any other institution with which the departing investigator or staff member will become affiliated;
- the feasibility of permitting the copying or removal of only de-identified, coded data, with the key to the code remaining at Yale;
- whether such copying or removal is contemplated in the Research Authorization signed by each subject;
- the feasibility of requesting additional Research Authorizations from the subjects;
- a review of any representations to, or agreements made by Yale with, the transferors of the data to Yale; and
- whether such copying or removal would be inconsistent with any representations made in the context of a waiver/decedents application.

The HIPAA Privacy Officer will then inform the departing investigator or research staff member of the terms and conditions under which research data may be copied or removed. Research data may be copied or removed from Yale *only* pursuant to those terms and conditions.

## **III. Patients' Rights Provisions in Research**

HIPAA gives patients certain rights with respect to their health information. In research that includes a treatment component, subjects have the right (1) to receive a Notice regarding Yale's Privacy Practices and (2) to access and amend their records. Subjects have the right to an accounting of disclosures of their PHI, regardless of whether or not the disclosures were related to treatment. For example, when conducting a study in which research results will be incorporated into subjects' permanent medical records, a

## Researchers' Guide to HIPAA Privacy

researcher must (1) provide the subjects with NOPPs and (2) address in the Research Authorization Form the issue of access to the medical records generated in the research study. When conducting studies that do not involve treatment, e.g., basic research involving healthy volunteers, researchers do not need to provide subjects with the NOPP or address in the RAF the research record access issue. However, in both of the types of studies described in the above examples, researchers must be able to provide an accounting of disclosures to subjects upon request.

### **Notice of Privacy Practices**

Under HIPAA, individuals have the right to receive adequate notice of (a) how Yale may use or disclose their PHI; (b) their rights under HIPAA; and (c) Yale's legal duties under HIPAA. This information is communicated via Yale's Notice of Privacy Practice (NOPP). <http://hipaa.yale.edu/>

Yale is required to provide a NOPP to any person with whom it has a direct treatment relationship and to any person who asks for a copy. Yale is also required to post the NOPP in a prominent location. The NOPP must be provided no later than the first date of service delivery.

Additionally, the institution, provider, or researcher must make a good faith effort to obtain the individual's written acknowledgement of receipt of the NOPP. Given that individuals need only be given one copy of a current or revised NOPP, investigators should verify that the subject has received the NOPP or provide the subject with a NOPP prior to commencing any research procedures. Patients of Yale School of Medicine (YSM) who receive the NOPP will be listed in IDX. Patients of Yale-New Haven Hospital (YNHH) who receive the NOPP will be listed in the SDK system, the data from which is periodically transferred to the YSM IDX system. Researchers should provide a NOPP to a subject whenever the subject's previous receipt of a NOPP cannot be verified through IDX or paper records. Most YSM business offices have access to IDX and can assist in verifying whether a subject has received the NOPP.

YSM and YNHH use a joint NOPP. The Yale School of Nursing and the Yale Psychology Department clinics each have their own NOPPs. Researchers should provide subjects with a copy of the relevant NOPP when required. For more information see <http://hipaa.yale.edu/>

### **Individual Right to Access and Amend**

HIPAA gives each patient the right to access and request amendment of his or her PHI that is maintained by Yale or its business associates in that patient's designated record set (DRS). Therefore, a patient has access to research information about him or her upon request if the research information is stored in the patient's DRS. The DRS includes any health information that was used to make a treatment decision, i.e., the patient's medical record.

Investigators conducting research that includes treatment can decide whether research notes will be included in the DRS. This is true only for data that is collected purely for

## Researchers' Guide to HIPAA Privacy

research purposes. Any data collected during a research study that is used for treatment decisions must be included in the DRS. If research records will be stored separate from the DRS, the storage must be done in such a way that the patient will not have access to edit the research record.

Researchers can deny subjects access to information contained in the research record or researchers can delay granting such access until after the study is completed. If researchers decide to restrict access during the course of the study, the restriction must be included in the Research Authorization Form. If researchers decide to delay granting access, then upon completion of the study, subjects may request and researchers must provide the subjects with a copy of their records.

Researchers should refer all subject requests for access to PHI obtained in the course of research to the appropriate Yale Records Department for processing in accordance with Yale policy. The policy is located at <http://www.yale.edu/ppdev/policy/5002/5002.html> and provides detailed guidelines for responding to such requests. The Records Department will determine, with assistance from the researcher and the HIPAA Privacy Officer, whether subject access to the PHI should be denied under established exceptions described in the policy.

### **Accounting for Disclosures**

Under HIPAA, patients have the right, upon request, to obtain a list of individuals or entities who have had access to or been provided with a copy of the patients' medical records for any reason other than treatment, payment, healthcare operations or with the patient's authorization. In order to meet this requirement, the medical record personnel responsible for a given record must maintain accounting logs for that record. The logs must include the names of those individuals who accessed the record, the reason for the access, and the date(s) the record was accessed. The entity responsible for the PHI must document a researcher's access to the record(s) at the time of access:

- under a waiver of Research Authorization,
- for recruitment purposes, and/or
- for research on decedents.

In order to minimize HIPAA violations and the burden on record holders, researchers may be asked to complete accounting logs for clinical departments or for YNHH. These logs may be stored with patient records or in an electronic database. When the researcher is also a treating clinician and the research use involves other members of a research team, the researcher must maintain the log.

Research records themselves are subject to HIPAA's accounting requirement when study PHI is:

- accessed for secondary data analysis by another researcher,
- accessed by additional researchers or entities not included in the Research Authorization Form signed by the subject, or
- disclosed in unanticipated events, e.g., theft or loss of records.

### **Record Retention**

HIPAA related documentation must be maintained for 6 years. This requirement applies to accounting for disclosures records, Research Authorization Forms, Data Use Agreements, and all other HIPAA forms.

If investigators request access to records for research purposes, they must provide the record holder with a "Request for Access to PHI for Research Purposes," IRB approval for the study, and any other relevant documentation outlined in the Request for Access form. This form must be maintained for the requisite six years.

Researchers should de-identify the data as soon as possible following completion of the study. If a researcher wishes to retain identified data after completion of a study, he or she must justify such retention to the IRB, and the IRB must approve the retention, including plans for securing the data.

## **IV. Privacy and Security Measures**

HIPAA requires that the privacy of PHI be maintained by limiting its uses and disclosures and that reasonable steps are taken to ensure that PHI is secure. Most often, breeches of privacy can be traced to lax security, so the two issues are intimately related. In April 2005, a portion of HIPAA known as the Security Rule became effective. The Security Rule requires institutions and individuals to take appropriate steps to secure the integrity, availability, and confidentiality of electronic PHI (ePHI). ePHI is defined as any PHI that is created, stored, accessed, or transmitted electronically. The Security Rule requirements apply to all electronic computing and communication systems that create, store, or transmit PHI, both on-campus and off-campus. All users, must comply with the Yale IT Appropriate Use Policy. The specific requirements for complying with the Security Rule can be found at <http://hipaa.yale.edu/security/>

Security requirements can change frequently and the web site should be referred to for the most recent policies and best practice guidelines. Some general guidelines to secure data include:

- Access to paper files should be limited by locking file cabinets or locking rooms with files
- Password protection of all computers using the ITS best practices for creating strong passwords
- PHI can not be transmitted using instant messaging or other insecure "Peer to Peer" software.
- Use of unencrypted e-mail to send PHI is limited in accordance HIPAA policy 5123 "Electronic Communication of Health Related Information" Note however that e-mail is allowed within or between Yale or Yale New Haven Hospital.
- Computing devices must be physically secured such as via use of locking cables for laptops or locking up storage devices such as memory sticks.

## Researchers' Guide to HIPAA Privacy

- Computing devices should be maintained with appropriate anti-virus and anti-spyware software.
- Databases containing PHI may also need an additional level of password protection to restrict access to the database itself and may need to be assessed via the ePHI tracking system.
- Disposal or re-use of electronic computing and communication devices requires that they be stripped of all PHI.
- Data should be routinely backed-up.
- Use secure network access procedures for connecting to the Yale network from off site locations.

## V. HIPAA in Research Contacts and Links

Human Investigation Committees (School of Medicine)

47 College Street, Suite 204

P.O. Box 208010

New Haven, CT 06520-8010

Phone: (203) 785-4688

Fax: (203) 785-2847

| <http://info.med.yale.edu/hic/>

Human Subjects Committee (Faculty of the Arts & Sciences)

155 Whitney Ave., Room 210

New Haven, CT 06520-8337

Phone: (203) 436-3650

Fax: (203) 432-4033

| [human.subjects@yale.edu](mailto:human.subjects@yale.edu)

<http://www.yale.edu/hsc/>

Human Subjects Research Review Committee (Yale School of Nursing)

100 Church Street South, Suite 200

P. O. Box 9740

New Haven, CT 06536-0740

Phone: (203) 737-2371

Fax: (203) 737-4480

| [sarah.zaino@yale.edu](mailto:sarah.zaino@yale.edu)

Yale University HIPAA Privacy Office

155 Whitney Ave., Room 210

New Haven, CT 06520-8337

Phone: (203) 436-3650

Fax: (203) 432-4033

[hipaa@yale.edu](mailto:hipaa@yale.edu)

Yale University HIPAA Web Site

| <http://hipaa.yale.edu/>

U.S. Department of Health & Human Services, Office of Civil Rights, (OCR)

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

U.S. Department of Health & Human Services, Office for Human Research Protections (OHRP)

| <http://ohrp.osophs.dhhs.gov/>

*This guidebook will be regularly updated. Please be sure to check the HIC and HIPAA websites at the URL listed above for the most recent copy.*

**Researcher Certification for HIPAA Privacy Rule Training**

**Compliance with HIPAA in Research Projects**

I understand that patient records, including demographic, biographic, insurance, financial, and clinical information, are confidential and are subject to the requirements of HIPAA and Yale policy. In the course of employment or association with a Yale University research project, I may need to access and review information contained in patient records, e.g., from file folders, computer display screens, and/or computer printers. I understand that I should access only the information that I need in order to perform my research related duties. If I encounter any additional patient record information, I will inform the principal investigator of the research study immediately.

Any release of this confidential information, either written or verbal, except as required in the performance of my research duties, is a violation of research conduct, and may be a violation of Yale policy and/or federal law. I understand that any such release may be considered reason for immediate termination and could result in civil and criminal penalties under the Health Insurance Portability and Accountability Act of 1996.

I have read and understand the Researchers' Guide to HIPAA and agree to the above statements.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Please print or type name

\_\_\_\_\_  
Home Institution

\_\_\_\_\_  
Research Project Title or HIC Protocol Number

\_\_\_\_\_  
Yale PI

**Forward to:**

HIPAA Privacy Office  
155 Whitney Ave, Room 210  
New Haven, CT 06520-8337  
Fax: 203-432-4033