

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

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

**Handbook**

**Table of Contents**

**I. Introduction**

- What is HIPAA?
- What is PHI?

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

- Requirements for Research Use of PHI
- Research Using or Creating PHI of Living Individuals
- Use/Disclosure of PHI in Approved Protocols
- 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
- Studies Exempted from IRB Review
- Databanks and Repositories
- 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 we 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 are limited to use and disclosure of Protected health information, or PHI. PHI is defined as individually identifiable health information that is created or received by a HIPAA covered entity.

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 of health care to an individual.

## Researcher's Guide to HIPAA

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

Covered entities are 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, School of Nursing, University Health Services, 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.

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

- The data includes any of the identifiers listed above AND
- Health information AND
- The data is created or received by YSM, YSN, YUHS, the Psychology Clinics or any other covered entity.

Procedures have been developed 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 eliminate the requirements of the 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 and disclosure of PHI for research purposes requires an authorization from the research subject unless some exception applies. HIPAA also applies to research related activities which were not covered under the Common Rule such as 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 not pursuant to an authorization to limit their access of PHI to only that needed to accomplish the research initiative and the intended purpose of the use and disclosure of PHI.

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

### **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

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

- Research using de-identified data
- Research conducted by an individual who is not part of a covered entity and that does not require access to information held by a HIPAA covered entity

Yale has developed a form which facilitates compliance and access by outlining the appropriate documentation or certifications required under HIPAA for access to PHI for research. The "Request for Access to PHI for Research Purposes" form should be completed and provided to the entity responsible for the PHI of interest along with the

## Researcher's Guide to HIPAA

documentation described on the form. The form has been approved for use by both Yale University and YNNH. Note that the form does not describe the requirements for access to a limited data set as this circumstance 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 conditions applies:

- Consents or Waivers of Informed Consent Obtained Prior to April 14, 2003
- Subject Authorization For Research
- IRB Approved Waiver of Authorization
- 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. An authorization form or request for a waiver is not required if subjects have executed an informed consent to participate 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 45CFR46.116(d).

If, after April 14, 2003, it becomes necessary to re-consent any participants in such studies, however, researchers are required to obtain a HIPAA compliant authorization or an approved request for waiver of 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 get 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 exercising the subject's rights related to the individual's protected health information. The written authorization must articulate:

- A specific description of what PHI will be used/disclosed.
- The names of persons or organizations who may use or disclose PHI.
- The names of persons or organizations to whom PHI will be disclosed.
- A statement of the purpose of the use/disclosure.
- A statement of how long the use 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 noted in the protocol).
- A statement that the authorization may be revoked.

## Researcher's Guide to HIPAA

- A statement regarding the potential for re-disclosure to others not subject to the Privacy Rule.
- A notice that the covered entity may or may not condition treatment or payment on the individual's signature.
- The individual's signature and 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 Authorization Form, the researcher should obtain another written authorization from the subject or apply for a waiver of authorization.

The [Yale University Research Authorization Form](#) has been designed to incorporate standard language for the statements required above. Investigators need only specify on the form to whom and where PHI will be sent and what type of PHI will be disclosed. Authorization forms which are not based on the Yale template or which 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 Document, 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).

Investigators should include the 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 authorization form, which acknowledges the IRB receipt and use of the form in research to comply with HIPAA regulations.

Copies of the signed 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.

### **Waiver of Authorization**

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

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

- The research could not be practicably conducted without the waiver.
- The research could not be practicably conducted without access and use of 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 study, or for other research for which the use or disclosure of protected health information would be permitted by the Privacy Rule.
- Uses and disclosures of PHI will be limited to the minimum necessary standard.
- Disclosure involves no more than minimal privacy risk to the individuals.
- Reviewed by the IRB with specific approval regarding access to the PHI.

## Researcher's Guide to HIPAA

Researchers can request a waiver of authorization by completing the [Yale University Request for HIPAA Waiver of Authorization for Research Form](#) and submitting to the IRB for 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 be practicably 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 statement regarding what PHI will be used and disclosed and that the PHI is limited to the "minimum necessary" standard.
- A statement that the disclosure involves no more than minimal privacy risk to the individuals.
- 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 are very similar to those for waiving informed consent. Therefore if the research plan includes obtaining informed consent from research participants, it is not likely that a waiver of HIPAA authorization will be granted, 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. It will be the responsibility of investigators to track 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. In most cases the request will be assessed utilizing an expedited review process. However, full IRB committee review is required in those instances where a waiver has been requested by the investigator but risk to the individual's privacy is considered to be greater than minimum. Investigators will receive from the IRB an authorized Approval/Denial of Waiver of HIPAA Authorization.

Copies of the waiver of 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**

PHI may be accessed 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. Summary data

## Researcher's Guide to HIPAA

(e.g., number of individuals with a certain disease) may be written down and removed. In addition, PHI may not be used to identify potential research subjects by name or by any other identifier under HIPAA.

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 preparatory activities using Yale University or Yale New Haven Hospital medical records can do so by completing 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. All requests for IDX reports should be forwarded 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 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 assurances 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 being sought.

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

### **Recruitment**

Under HIPAA, 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 only require access to a limited amount of health information, recruitment nonetheless is considered to be accessing 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.

## Researcher's Guide to HIPAA

- 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 the information to a researcher when the researcher has obtained an approved Waiver of Authorization from an IRB for recruitment purposes.

A blanket Research Authorization for recruitment purposes is not permissible. Thus, a researcher may **not** ask a patient to sign an authorization permitting the researcher (or anyone else) to contact the patient for future unspecified studies.

HIPAA also applies to recruitment and research activities conducted via medical records and medical registry reviews. Investigators must obtain either 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 a subjects authorization 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 [HIPAA Authorization Form](#) or Requests for Waiver of HIPAA Authorization that will be used after recruitment and submit it to the IRB as described in the previous section on waivers.

### **De-identified Data**

De-identified data are data that contains none of the 18 identifiers listed earlier. If all of the identifiers are removed, the information is considered to be no longer individually identifiable, no longer PHI, and no longer subject to HIPAA's requirements. A de-identified data set may be coded with a unique identifier that cannot be traced back to 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 resubmission of the protocol to the IRB for approval is required 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 presents a very small risk that the information can be used alone or in combination with other reasonably available information to identify an individual.

### **Limited Data Set**

Some studies may need some limited identifiers and thus not meet the strict definition of "de-identified data" but nonetheless hold only minimal potential for identifying

## Researcher's Guide to HIPAA

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 Photo                    |

A limited data set may include one or more of the following:

- |  |
|--|
| 1. Town  |
| 2. City  |
| 3. State   |
| 4. Zip Code and their equivalent geocodes. (Note the zip code cannot be used if the area composing the zip code has less 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  |

A limited data set may only be used for purposes of research, public health, or health care operations. It may only be used 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.

As with research conducted pursuant to an authorization, disclosures of PHI that is 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 further state that the research activity cannot begin until the principal investigator has an authorized Data Use Agreement in place.

*Other resources providing information on de-identification and Limited Data Set Procedures include:*

## Researcher's Guide to HIPAA

*Yale University Policy regarding the Use and Disclosure of De-Identified Information and of Limited Data Sets at <http://hipaa.yale.edu/>.*

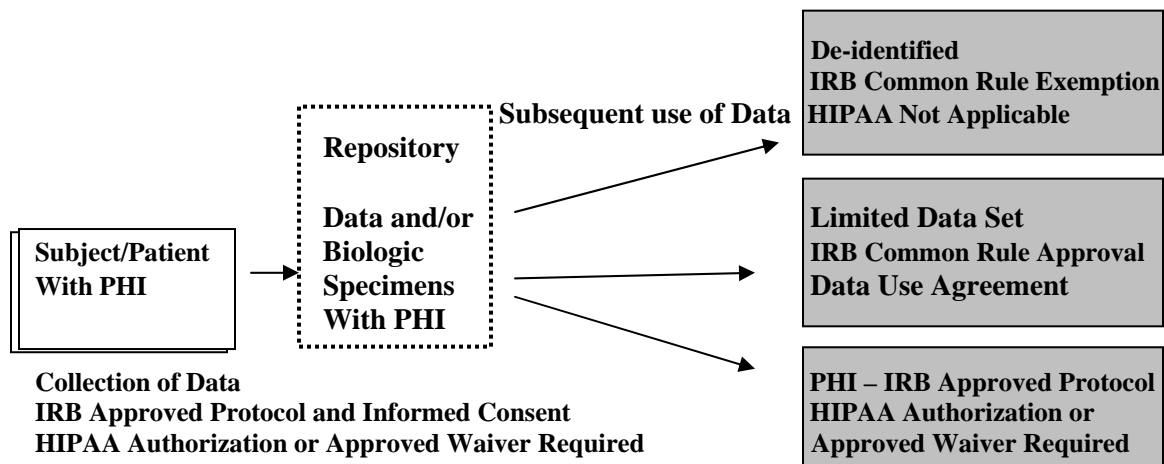
*Yale University Procedure on De-Identification and Limited Data Set Procedures at <http://info.med.yale.edu/hic/> or Contact the Privacy Officer for more information.*

### **Databanks and Repositories**

Investigators are reminded that the collection or maintenance of PHI in databanks or repositories for future research purposes requires an IRB approved protocol. Similarly, research utilizing data from these databanks and repositories must be conducted under a protocol approved by the IRB. Since databanks and tissue repositories frequently survive the lifespan of the initial IRB protocol from which the data/tissue is collected, it is recommended that the banking be submitted to the IRB as 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 IRB for the collection of PHI and prior to conducting subsequent studies utilizing PHI.

Authorizations for tissue banking generally will become part of the individual's medical record. As such, the use of a compound authorization (eg consent plus authorization combined) is not appropriate as the consent usually contains additional information which may not be appropriate in the permanent medical record.



### **Studies Exempted from IRB Review**

Studies which have been exempted under the Common Rule but which involve the use of PHI are not also exempted under HIPAA. HIPAA requirements related to authorization

## Researcher's Guide to HIPAA

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.

### **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 by Yale, he or she must request permission from his or her department chair and the Privacy Officer. Taking the data to a new institution constitutes a disclosure of PHI under HIPAA and necessitates that the disclosure be tracked in the accounting for disclosures log. The Privacy Officer will make each determination related to privacy rules on a case-by-case basis, considering at least the following:

- does the data include PHI;
- who, besides 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 authorizations from the subjects;
- 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 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. Patient's Rights Provisions in Research**

HIPAA mandates certain rights to patients with respect to their health information. The right to notice regarding our privacy practices and the right to access and amend their records are applicable to research which also includes a treatment component. The right to an accounting of disclosures applies to all PHI, whether treatment related or not. For example, studies where research results are incorporated into a subjects permanent medical record would need to provide a Notice of Privacy Practices and address access to the medical records generated in the research study in the Research Authorization Form. Studies which do not involve treatment, such as basic research involving healthy volunteers would not need to provide the notice or access to records. Both examples would need to be able to provide an accounting of disclosures 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, to any person who asks for it, and it must also post the NOPP in a prominent location. Beginning April 14, 2003, the Notice must be presented 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 provided with 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 research procedures. Patients of YSM receiving the NOPP will be listed in IDX. Patients of YNHH receiving the NOPP will be listed in the SDK system. Plans are underway to populate the NOPP information from the University's IDX system into the hospital's SDK system. Researchers are reminded that NOPPs should be distributed in those instances where previous receipt of the NOPP by the patient cannot be verified through IDX or paper records. Most YSM business offices have access to IDX and could assist in verifying a subject's prior receipt of the NOPP.

Note that Yale School of Medicine and Yale-New Haven Hospital will be using a joint NOPP. Yale School of Nursing and the clinics of the Psychology Department each will have their own NOPPs. Researchers should provide subjects with a copy of the relevant NOPP when required. <http://hipaa.yale.edu/>

### **Individual Right to Access PHI**

HIPAA provides individuals with the right to access and request amendment of the PHI that is maintained by Yale or its business associates in the patient's designated record set (DSR). Thus, patient access to research information is available upon request if research information is stored in the designated record set. The designated record set includes any health information which was used to make a treatment decision, generally speaking the patient's medical record.

Investigators or departments conducting research in conjunction with treatment are given the option to determine whether research notes are included into the designated record set. This option only holds for data, which is collected purely for research purposes. Thus data collected during a research study, which is used for treatment decisions, would be included in the DSR. If research records are stored separately, it must be done in such a way that the patient does not have access to edit the research record.

Researchers can deny subject access to information contained in the research record or delay granting access until after study is complete. If access is to be restricted for the

## Researcher's Guide to HIPAA

course of the study, this restriction must be indicated in the research authorization form. Upon completion of the study, participants may request and be provided with a copy of their records.

All requests for access to PHI obtained in the course of research should be referred to the appropriate Records Department, if applicable, for processing in accordance with Yale policy. The policy can be found 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 Privacy Officer, whether access to PHI should be denied under certain established exceptions described in the policy.

### **Accounting for Disclosures**

HIPAA requires that, upon request, patients be provided with a listing of who has had access to or been provided a copy of their records for reasons other than treatment, payment, healthcare operations or with the patient's authorization. In order to meet this requirement, accounting logs must be maintained by the medical record personnel responsible for the record which include who had access, for what reason and when access was provided. The entity responsible for the PHI must document researcher's access to the records when it is performed:

- under a waiver of authorization
- for recruitment purposes
- for research on decedents

In an effort to minimize the burden on the record holders and to minimize research use leading to HIPAA violations, researchers may be asked complete accounting logs for clinical departments or YNHH. These logs may be stored with the 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 will need to maintain the log.

Research records themselves are also subject to the accounting requirement when study PHI is:

- accessed for secondary data analysis by another researcher
- accessed by additional researchers or entities not included in the authorization form signed by the subject
- disclosed in unanticipated events such as theft or loss of records.

### **Record Retention**

HIPAA related documentation must be maintained for 6 years. This requirement applies to accounting for disclosures records, authorizations, data use agreements and any other HIPAA forms.

If the records are maintained and access to them is requested for research, note that the "Request for Access to PHI for Research Purposes" will need to be collected from the

## Researcher's Guide to HIPAA

individual who wishes to make use of the records along with the IRB approval and other relevant documentation as outlined in the Request Access form. This form will need to be maintained for the requisite six years.

The data itself should be de-identified as soon as possible following the completion of the study. If the retention of identified data is contemplated, such retention must be justified and approved by the IRB, including plans for securing the data.

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

HIPAA requires that we maintain the privacy of PHI by limiting its uses and disclosures and that we take reasonable steps to ensure that the PHI is secure. Most often, breeches in privacy can be traced to lax security so the two issues are intimately related.

Some steps 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
- Databases containing PHI may also need an additional level of password protection to restrict access to the database itself
- Avoid sending PHI in e-mail or as e-mail attachments. If an attachment must be used, the attachment can be password protected and possibly may require encryption depending on the sensitivity of the data.

### **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 214,

New Haven, CT 06520-8337

Phone: (203) 436-3650

Fax: (203) 432-7138

[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

## Researcher's Guide to HIPAA

New Haven, CT 06536-0740

Phone: (203) 737-2371

Fax: (203) 737-4480

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

University Privacy Office

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 website at the URL listed above for the most recent copy. 325*

Researcher's Guide to HIPAA

**Researcher Certification**

**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. In the course of employment or association with a Yale University research project, this information may be required and consequently accessed from file folders, computer display screens, and computer printers. I understand that I should only access that information which I need to perform my research related duties.

Release of this confidential information, either written or verbal, except as required in the performance of research, is a critical violation of research conduct. As such, it 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 Researcher's 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 300B  
P.O. Box 208252  
New Haven, CT 06520-8252  
Fax: 203-432-4033

Version 08/2009