YALE UNIVERSITY
RESEARCHER'S GUIDE TO HIPAA

Health Insurance Portability and Accountability Act of 1996
Handbook

Table of Contents

I. INTRODUCTION 2
What is HIPAA? 2
What is PHI? 2
II. HIPAA's IMPACT ON RESEARCH PROTOCOLS 3
Requirements for Research Use of PHI 4
Research Using or Creating PHI of Living Individuals. 4
Consent or Waiver Obtained Prior to April 14, 2003 5
Research under a Participant's Authorization 5
Waiver of Authorization 6
Activities Preparatory to Research 7
Research on Decedents 7
Recruitment 8
De-identified Data 9
Limited Data Set 9
Databanks and Repositories 10
Studies Exempted from IRB Review 11
Resignations of Investigators or Research Staff 11
III. Patient's Rights Provisions in Research 11
Notice of Privacy Practices 12
Breach of PHI 12
Individual Right to Access PHI 12
Accounting for Disclosures 13
Record Retention 14
IV Privacy and Security Measures 14
V. HIPAA In Research Contacts and Links 17
VI Researcher Certification 18

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, health care operations or those of an electronic health record). If you need guidance on these issues, please refer to http://hipaa.yale.edu/.

What is PHI?

HIPAA's privacy 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.

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 (excluding the School of Public Health, the Animal Resources Center, and the basic science departments: Cell Biology, Cellular and Molecular Physiology, Comparative Medicine, History of Medicine, Immunobiology, Microbial Pathogenesis, Molecular Biophysics & Biochemistry, Neurobiology, Pharmacology and WM Keck Biotechnology Resources Laboratory), School of Nursing, Yale Health, 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 most of the Faculty of Arts and Sciences, are not subject to HIPAA. Although not everyone in clinical departments at 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.

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

Note that identifiers that are obtained from Yale's clinical system are considered to include health information based on the implicit understanding that to be listed in our clinical systems indicates that care was or will be provided.

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 a clinical department in YSM, YSN, Yale Health, the Psychology Clinics or any other covered entity

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 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 who have been deceased for less than 50 years 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 who have been deceased less than 50 years
- 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
- Research on individuals who have been deceased more than 50 years

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 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. Where access will be electronic, the form certifying that the relevant HIPAA requirements are met should be retained with study records for at least 6 years.

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:

- Consent 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 or Waiver Obtained Prior to April 14, 2003

Researchers may continue to use or disclose PHI obtained or create 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.

Under HIPAA the consent form and HIPAA Research Authorization form (RAF) can be combined for the same study, e.g., a single research purpose into what is referred to as a "Compound Authorization". By combining the consent and the authorization form, we can be assured that both HIPAA and Common Rule requirements are met. Use of a compound authorization is the standard practice here at Yale. However, the two documents are not required to be combined and in some cases the researcher may have reason to separate the two documents.

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.
- 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 individuals or groups 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.

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).

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, where feasible. Otherwise, the form should be stored with the research records for at least 6 years.

Waiver of Authorization

If the research study involves PHI and certain other conditions exist, the researcher may request in their IRB protocol, 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 to 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.

Researchers can request a waiver of authorization by completing the appropriate section of the IRB application 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 https://hipaa.yale.edu/sites/default/files/files/5003-PR-5003-PR1.pdf)* 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 where feasible. Otherwise, the form should be stored with the research records for at least 6 years.

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 (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. Once completed the certification should be stored with the research records for at least 6 years.

Clinical administrators should not run reports out of EPIC for research purposes.
All requests for Epic reports are handled by The Joint Data Analytics Team (JDAT). For information and the process for requests for data for researchers from Epic see:
https://medicine.yale.edu/ycci/researchers/datarequests.aspx

Research on Decedents

HIPAA requires that researchers who wish to access PHI of decedents who have been deceased less than 50 years first make certain representations to the holder of the PHI. The Health information of

individuals who have been deceased for more than 50 years is not subject to the HIPAA requirements. 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. Once completed the certification should be stored with the research records for at least 6 years.

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.
- 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.

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 subject's authorization after recruiting and enrolling subjects via a partial waiver and prior to creating or using PHI during research procedures.

Investigators should include a request for HIPAA waiver of authorization within 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 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.

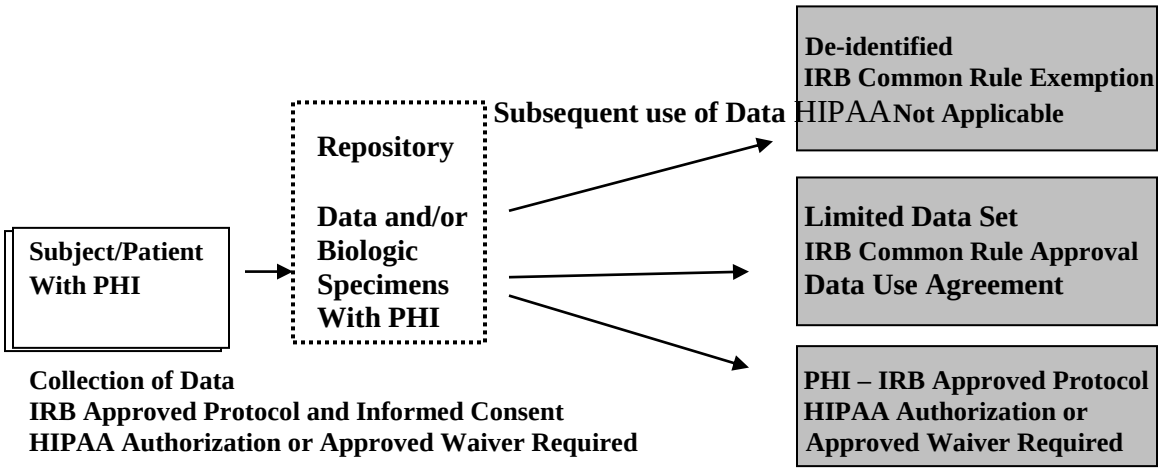
The use of a Limited Data Set in a protocol should be specified in the research plan and confidentiality sections. The IRB will acknowledge the use of the Limited Data Set in the IRB approval letter sent to the principal investigator. The letter will further state that the research activity cannot begin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

Procedures related to de-identification and Limited Data Set Procedures may be found at: https://hipaa.yale.edu/sites/default/files/files/5039-PR.pdf

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. HIPAA allows combining the consent and authorization for a study with authorization for the creation or maintenance of a research database or repository. Combining study authorization with database or repository authorization requires that these distinct uses must be clear and allow for the research subject to provide separate authorization for the database or repository. Example: the subject is given the option to provide permission for sharing information for purposes related to the trial AND in a separate statement, the subject provides a “second” permission to bank the biologic material for use in future research studies. If selecting this option, investigators are reminded to retain the signed combined form for the full duration that the banked data or biologic sample will be retained for future research purposes.



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 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 in accordance with University Research Data and Materials Policy (see https://research.yale.edu/sites/default/files/files/Research%20Data%20Policy%2009-14-2017.pdf) and IRB Policy 730 (https://research.yale.edu/sites/default/files/files/Research%20Data%20Policy%2009-14-2017.pdf).

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. Accounting logs must be completed by the research team and submitted to the HIPAA Privacy Office. For further information on accounting of disclosures see: https://hipaa.yale.edu/sites/default/files/files/5003-PR-5003-PR1.pdf

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 subject's 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. 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 or YNHH receiving the NOPP will be listed in EPIC. Researchers are reminded that NOPPs should be distributed in those instances where previous receipt of the NOPP by the patient cannot be verified through EPIC or paper records. Most YSM business offices have access to EPIC and could assist in verifying a subject's prior receipt of the NOPP.

Note that Yale School of Medicine, Yale School of Nursing and Yale-New Haven Hospital will be using a joint NOPP. 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/

Breach of PHI

Patients have a right to be notified in cases where their PHI has been inappropriately accessed, used or disclosed in violation of the Privacy Rule. Potential breaches include lost paper records, lost smartphones or laptops containing PHI, misdirected mail, email or faxes etc.

Notify Yale IMMEDIATELY of all events that might be potential breaches!

Call 203-627-4665 if you believe ePHI/PHI might have been lost, stolen, compromised, misdirected, etc. Yale HIPAA professionals will work with you to determine the next steps, and whether the event requires notification.

Anyone else wishing to report a HIPAA concern should call 203-432-5919 or email 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.

Researchers can deny subject access to information contained in the research record or delay granting access until after the study is complete. If access is to be restricted for the 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 https://hipaa.yale.edu/sites/default/files/files/5002-PR-5002B.pdf 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 individuals external to the HIPAA covered entity who have 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 to 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 of disclosure to individuals not associated with the Yale covered entity (eg individuals outside of Yale School of Medicine (Excluding the School of Public Health, the Animal Resource Center, and the basic science departments: the Departments of Cell Biology, Cellular and Molecular Physiology, Comparative Medicine, History of Medicine, Immunobiology, Microbial Pathogenesis, Molecular Biophysics & Biochemistry, Neurobiology, and Pharmacology), School of Nursing, Yale Health, and the Department of Psychology Clinics.

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

- accessed for secondary data analysis by another researcher outside the Yale HIPAA covered entity
- 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 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 take reasonably steps to ensure that the PHI is secure. Most often, breaches in privacy can be traced to lax security so the two issues are intimately related. PHI is considered high risk data. For more information on Data Classification and Approved Services/Vendors for high risk data see: https://your.yale.edu/protect-your-data.

Key security requirements are outlined below. Note that security requirements change frequently and users are advised to review the information at https://hipaa.yale.edu/security for the most recent requirements.

1. Everyone must complete Yale's HIPAA Privacy and Security training (https://hipaa.yale.edu/training/training-modules) and understand Yale's Policy 5100 Electronic Protected Health Information (ePHI) Security Compliance: HIPAA Security Anchor Policy

2. Everyone must use "strong" passwords (8 – 14 characters, with at least two letters and two non-letters) for computer and application access and must comply with ITS password security standards (https://your.yale.edu/policies-procedures/guides/1610-gd01-selecting-good-passwords).

3. Everyone must secure paper records that include PHI as required by Yale policy https://hipaa.yale.edu/security/policy-guidelines-physical-security

4. Everyone must immediately report incidents that may involve a breach of PHI or ePHI to **(203) 627-4665** for ePHI or **hipaa@yale.edu** for PHI.

5. Everyone must attest annually to full compliance with HIPAA policies at: https://bmsweb.med.yale.edu/tms/tms_enrollments.offerings?p_crs_id=2448&p_std_id=#

6. You may not acces or store ePHI on personally owned computers unless an exception applies such as Citrix access to Epic. If remote access to on-campus workstations or systems (e.g., Yale email) is needed a University-provided, fully managed and encrypted device with VPN must be used.

7. You must ensure that the following security measures have been applied to all Yale laptop and desktop computers you use to store, access, transmit or receive ePHI:

    a. Encryption – Whole disk encryption utilizing either Microsoft BitLocker or Apple FileVault This includes any external storage device used to transport Yale data.

    b. Administrator Privileges – Removal of administrator privileges.

    c. Registration - Register all systems (e.g. desktops, laptops, clinical devices, etc.) in the Yale IP Address Management System.

    d. Network Address - Private IP addresses shall be used on all systems (e.g. desktops, laptops, clinical devices, etc.).

    e. Identification – All systems employ IBM Endpoint Manager for identification purposes.

    f. Operating System – Operating Systems are to be in compliance with the published "Yale Standard Supported Operating Systems."

    g. Patching - Automatic distribution of security and other patches via central computer management software (IEM Endpoint Manager is recommended).

    h. Anti-Virus Protection - Installation and update of managed anti-virus/anti-spyware software.

    i. Enterprise Directory - Configure all systems (e.g. desktops, laptops, clinical devices, etc.) to be on the Yale domain.

    j. Enterprise Authentication - All system (e.g. desktops, laptops, clinical devices, etc.) logon requests will need to utilize Yale credentials and will need to be processed through Yale's enterprise directory.

    k. Backup – Registration in the ITS Crashplan backup service.

    l. Inactivity Lock - Automatic locking and password protection of systems after 15 minutes of inactivity.

    m. Application Security - Removal of applications that increase the vulnerability of computers such as Peer to Peer (P2P) file sharing.

    n. External Messaging Applications – Yale business must be conducted only on Yale-approved instant messaging applications.

    o. Procurement - Purchase all new desktop and laptop computers from Yale's Managed Workstation portfolio (located in SciQuest).

    p. Other – Additional safeguards as they become technically feasible.

Up-to-date secure workstation configuration standards are located at https://your.yale.edu/work-yale/data-security/minimum-security-standards

8. You must ensure that the following security measures have been applied to smartphones, tablets, and similar devices (collectively "mobile data devices") that you use to create, store, access, transmit or receive ePHI, whether the devices are Yale-issued or personally owned:

    a. Passwords: You must use a password with a minimum of four characters. Your mobile data device must be set to delete all data or lock internally after 10 unsuccessful attempts to enter a password.

    b. Encryption: The data on your mobile data device must be encrypted.

    c. Message Storage Limits: You may not store more than 200 messages or 14 days of messages on your mobile data device.

    d. Applications: Applications that create, store, access, send or receive ePHI must meet Yale security standards. Please contact information.security@yale.edu for additional information.

    e. Software: You must keep software patched and up to date.

    f. Tracking and remote deletion enrollment: Your mobile data device must be capable of remote deletion and locking using your Yale Connect account or subscribe to a service that allows remote deletion of messages in the event it is lost or stolen.

    g. No circumvention of device security: You must not circumvent the security of your mobile data device by removing limitations designed to protect the device ("jailbreaking"), and you must not tamper with your device by using unauthorized software, hardware, or other methods.

    h. Safe wireless data networking:. You must use Yale's VPN services if you connect to the Yale network from a mobile data device and are not using one of Yale's cellular carriers (for example, if you are using "roaming" mode internationally). For WiFi networking, you may use only secure (WPA-2) WiFi networks known to be trustworthy (such as "Yale Secure"). Bluetooth™: Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices.

    Up-to-date ITS mobile data device standards and information on how to comply are located at https://hipaa.yale.edu/security/breach-prevention/smartphones.

9. You may never store ePHI on thumb drives or other portable media devices, unless they meet Yale ITS encryption standards (https://its.yale.edu/secure-computing/security-standards-and-guidance/data-and-application-security/protecting-yales-data/data-encryption

10. If you must forward or exchange ePHI data files or datasets outside the University or YNHH networks, you must use the ITS Secure File Transfer Facility. https://its.yale.edu/services/communication-and-collaboration/document-sharing-and-team-sites/secure-file-transfer-facility

11. You are required to use ITS-managed servers for storage of ePHI whenever any one of the following conditions apply:

a. You are storing the ePHI of 500 or more patients;
b. Access to the ePHI is shared by more than one user;
c. The files containing the ePHI comprise 500 GB of data or more.

Exceptions must be approved by the Yale Information Security Policy and Compliance Office.

12. Reasonable and appropriate physical security must be implemented to secure computing devices housing ePHI including:

a. Privacy filters must be installed on computer screens that display ePHI and can be viewed by the public or non-clinical staff.

b. Whenever possible, the space must be secured through locking the room or area when a computer will be unattended for extended periods since physical access to your computer allows other methods of access to your data (e.g. inserting a disk or CD with tools for "hacking"

c. A locking cable or equivalent physical protection (e.g. locked cabinets) for all devices when not in the user's physical custoy.

13 You must securely destroy or delete paper PHI or ePHI when no longer needed or when retiring computers, smartphones or other mobile devices such as thumb drives. Please refer to Procedure 1609 PR.01 Disposal of Media Containing Confidential or Protected Health Information:

14 You must not configure Yale email accounts that may receive or transmit ePHI to auto-forward messages to non-Yale email accounts(e.g. Google. Yahoo, Hotmail).

15. ePHI may not be stored on any commercial data storage service unless the service has been approved by ITS and has signed a Business Associate Agreement with Yale. Under no circumstances may ePHI be stored on a personal Internet-accessible data storage device.

V. HIPAA In Research Contacts and Links

Human Research Protection Program
25 Science Park
150 Munson St. 3rd floor
P.O. Box 208327
New Haven, CT 06520-8327
(203) 785-4688
http://www.yale.edu/hrpp/
hrpp@yale.edu

University HIPAA Privacy Office
2 Whitney Ave, Suite 204
PO Box 208255
New Haven, CT 06520
(203) 432-5919

http://hipaa.yale.edu
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://www.hhs.gov/ohrp/

Yale Requirements related to HIPAA Privacy Training

I understand that patient records including demographic, biographic, insurance, financial, and clinical information are confidential. In the course of employment or association with the Yale University, 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 work related duties and that my access to the system may be monitored electronically.

Release of this confidential information, either written or verbal, except as required in the performance of work, is a critical violation of employee conduct. As such, it may be considered reason for immediate termination of employment and could result in civil and criminal penalties under the Health Insurance Portability and Accountability Act of 1996.

Yale Requirements related to HIPAA Security Training

The HIPAA Security Rule also requires that all individuals in the covered entities who handle protected health information in an electronic form complete training on the requirements of the Security Rule. Yale University policy also requires that all within the covered entity departments who use computing or communications systems during the course of work, complete the online HIPAA Privacy and Security training.

HIPAA Privacy and Security Training Certification

By signing below, I certify that:

- ☐ I have read and understand the Researcher's Guide for HIPAA Privacy Training and agree to the above HIPAA Privacy Training statements.

AND

- ☐ I do NOT create, receive, maintain or transmit Protected Health Information in an electronic form or provide IT support to someone who does in the performance of my University appointment.

AND

- ☐ I do NOT use computing or communications systems during the course of my work at the School of Medicine, School of Nursing or the University Health Plan. This includes Systems use on-campus as well as from remote locations, such as home, hotels and other off-campus locations and the use of a Yale e-mail account.

_____	_____
Signature	Date
_____	_____ Please
Print or Type Name	Yale NetID
_____	_____
Department Name	Supervisor's Name
_____	_____
Job Title	Lead Administrator's Signature

Forward to: HIPAA Privacy Office, P.O. Box 208255, New Haven, CT 06520-8255; Fax: 203-432-4033; hipaa@yale.edu