Introduction

What is HIPAA?

HIPAA stands for 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).
Not all of Yale is subject to the regulation. HIPAA applies to School of Nursing, Yale Health, the Department of Psychology Clinics and 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).

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.

The HIPAA Security Rule:

- Establishes administrative, technical and physical standards for the security of electronic protected health information (ePHI);
- Requires that we maintain the availability, integrity, and confidentiality of electronic health information.

The HITECH Act

- The Health Information Technology for Economic and Clinical Health (HITECH) Act amended HIPAA, including the addition of a requirement to notify patients and the US Department of Health and Human Services in the event of a breach of PHI.

This guide addresses the HIPAA Privacy Rule's requirements, as amended by the HITECH Act, related to uses and disclosures of PHI for clinicians working at Yale. If you need further guidance on HIPAA or information related to the Security Rule, please refer to http://hipaa.yale.edu/.

Health Information Privacy

Privacy refers to an individual's right to control access and disclosure of their individually identifiable health information. HIPAA requires that information provided by the patient to health care providers including notes and observations about the patient's health will not be used for purposes other than treatment, payment, health care operations or for the specific purposes described in the Privacy Rule.

The Privacy Rule does not prevent physicians from discussing patient information with fellow providers for treatment purposes. In other cases, such as securing payment or conducting audits, the regulations require providers make a reasonable effort to disclose only that information which is necessary for that purpose.

Protected Health Information

Protected Health Information (PHI) under HIPAA means any information that identifies an individual **and** relates to at least one of the following:

- The individual's past, present or future physical or mental health.
- The provision of health care to the individual.
- The past, present or future payment for health care.

Information is deemed to identify an individual if it includes either the individual's name or any other information that could enable someone to determine the individual's identity (e.g., address, age, Social Security number, e-mail address). For a complete definition of PHI and other HIPAA terms see the HIPAA glossary at hipaa.yale.edu

Identifiers

Data are "individually identifiable" if they include **any** of the 18 types of identifiers, listed below, for an individual or for the individual's employer or family member, **or** if the provider or researcher is aware that the information could be used, either alone or in combination with other information, to identify an individual:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city, county, ZIP code)
- All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89)
- Telephone numbers
- FAX number
- E-mail address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Device identifiers or serial numbers
- Web URL
- Internet Protocol (IP) address numbers
- Finger or voice prints
- Photographic images

- Any other characteristic that could uniquely identify the individual

Note that identifiers alone, when they are derived from any of our clinical systems, are considered PHI as inclusion in our systems is indicative of having received treatment or payment for treatment and as such must be afforded the same protection as more detailed information.

HIPAA's Impact on Clinical Practice, Treatment, Referrals and Payment

How is Protected Information Used?

Information that Yale collects or creates that relates to patient health or to patient care can only be used in limited ways without patient authorization.

Patient authorization is not required when doctors, nurses, therapists, dieticians, and others use information about patients to determine what services they should receive or to review the quality of their care. PHI may also be used without patient authorization to bill patients (or their insurance companies) for the services they received or to fulfill other necessary administrative and support functions.

Disclosure is also permitted without authorization in a number of other situations, such as where disclosures are required by law. Below is a list of some common situations where PHI can be released without a patient's authorization:

Reasons for Releasing PHI

There are certain situations in which Yale may release PHI without the patient's authorization. These include:

- Providers are required to report certain communicable diseases to state health agencies, even if the patient doesn't want the information reported.
- The Food and Drug Administration requires that certain information be reported about medical devices that break or malfunction.
- The courts have the right to order providers to release patient information with appropriate certifications or court orders.
- Under limited circumstances, health care providers may disclose PHI to police (such as reporting certain wounds or injuries, or to comply with a court-ordered warrant or grand jury subpoena).
- When physicians or other people providing patient care suspect child abuse or elder abuse, they must report it to state agencies.
- The hospital or provider reports information to coroners and funeral directors in cases where patients die.

Patients can also request release of their information by signing an authorization which includes all the statements required under the regulations. Use of the Yale University

Authorization for Use and Disclosure of PHI (form 5031) meets the regulatory requirements. When responding to an authorization from another organization for release of protected health information, the authorization must also meet the HIPAA requirements. If there is any doubt, the Privacy Office can provide assistance in reviewing the validity of the document.

Psychotherapy Notes

Psychotherapy notes receive stronger protection than other protected health information under the HIPAA privacy rule because of their potential sensitivity. Psychotherapy notes are defined as the notes of a mental health professional which document or analyze the contents of a counseling session and which are stored separately from the rest of the medical record. Except in certain limited circumstances, use or disclosure of psychotherapy notes is permissible only if the patient signs a separate authorization that encompasses *only psychotherapy notes* and no other PHI.

Psychotherapy notes exclude:

- Medication prescription and monitoring
- Counseling session start and stop times
- Modalities and frequencies of treatment furnished
- Results of clinical tests
- Any summary of diagnosis, functional status, treatment plan, symptoms, prognosis, or progress to date

Using Information for Marketing Purposes

Yale can continue to communicate with our patients concerning the health care services we provide without obtaining patient authorization. For example, a clinical department may describe the health care services it offers, or a clinician may recommend treatments, therapies or other health care providers in the course of treating a patient. Similarly, a marketing authorization is not needed to inform patients of a new service or health care program or of a change in office location.

However, the HIPAA privacy rule does not allow us to disclose PHI to another organization for that organization's marketing purposes unless the patient authorizes that disclosure.

Fundraising

Yale may use only limited protected health information for its own fundraising efforts such as demographic information, name of treating clinician and department of service. Demographic information includes names, addresses and other contact information, age, gender, and insurance status.

All fundraising communications must offer the individual and easy way to opt out of receiving any further fundraising communications. If someone opts out, we are required to honor that request. If a patient requests to not be included in future fundraising

solicitations, the request should be forwarded to the Development Office for inclusion on the opt-out list.

Patient's Rights

Notice of Privacy Practices

The Notice of Privacy Practices (NOPP):

- Explains privacy policies
- Explains how patient information will be used
- Informs patients about their rights

Who receives the NOPP?

- First time patients
- Research subjects in a study that is also providing clinical care
- Anyone who requests a copy

Patients must be asked to sign an acknowledgement of receipt, although they are not required to sign it. The NOPP must be posted prominently in patient areas.

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.

Individual Right to Access and Amendment

Patients have a right to inspect and be provided a copy, either on paper or an electronic copy, of their health information that is maintained in their designated record set (definition below). The patient is required to either write a letter or fill out a form to request access and we must provide access within 30 days. Patients can also request amendments to their medical records. Note that Yale staff who are also Yale patients and who have access to the electronic medical record in the course of their work, may use that access to view and print their own records. Staff may not use their work-related access to view or print records of any other individuals, including family members, other than as required in the performance of their Yale related duties.

Designated Record Set

A designated record set is comprised of the following documents which are part of the patient's permanent medical record:

- Advance Directives
- Consents and Authorizations
- Consultations
- Correspondence and Calls recorded in the medical record
- Demographic information
- Diagnostic Imaging Reports
- Discharge Instructions
- EEG Reports
- EKG Reports
- Forms that are included in the permanent record
- Graphic and Flow Sheets
- History, including past Medical and Surgical History
- Home Health Documentation
- Identification Sheet/Face Sheet
- Immunization Records
- Laboratory Reports
- Medical Release Forms
- Medication Records
- Nursing Documentation
- Notes
- Pathology Reports
- Photographs (if included in the medical record)
- Physical Exam
- Problem List
- Progress Notes (including interdisciplinary documentation)
- Reports of Operations/Procedures
- Scanned documents
- Therapy Reports
- (Past) Medical records archived electronically or stored in paper or other media
- Requests for Amendment
- Amendments
- Denials of Requests for Amendments

The following documents that are part of billing records retained for patients are also included in the designated record set.

- Life Time Insurance Authorization (LTIA) (scanned image)
- Medicare Advanced Beneficiary Notice
- Payment Agreement

- Requests for Amendment
- Amendments
- Denials of Requests for Amendments

Accounting for Disclosures

HIPAA requires that, upon request, patients be provided with a listing of individuals outside the Yale HIPAA Covered Entity who have had access to or been provided a copy of their records (1) for reasons other than treatment, payment, healthcare operations or (2) without the patient's authorization. In order to meet this requirement, accounting logs must be maintained by the medical record personnel responsible for the record. The logs must include who had access, for what reason and when access was provided. This requirement also holds true for research access to PHI when access is granted to researchers not affiliated with Yale or Yale New Haven Health under a waiver of authorization, for recruitment purposes or for research on decedents.

Operational Procedures for Protecting Privacy

The "Minimum Necessary" Standard

Medical staff must make a reasonable effort to disclose or use only the minimum necessary amount of protected health information in order to do their jobs. They can disclose information requested by other health care providers if the information is necessary for treatment.

Physicians and providers who are directly involved in the care of the patient can see PHI. Providers can disclose to consulting physicians or for referrals, but not to people who don't have clinical responsibilities. Physicians must be careful about what they disclose to other staff members, such as billing department workers or providers not involved in the care of their patient.

Making "minimum necessary" determinations is a balancing act. Providers must weigh the need to protect patients' privacy against their reasonable ability to limit the information that is disclosed while delivering quality care.

Everyday Steps for Protecting Privacy

Here are some common ways that clinical staff members can protect patient privacy:

- Talk on the phone in closed quarters, and be careful what you disclose aloud
- Close patient room doors when discussing treatments and administering procedures. Close curtains and speak softly in semi-private rooms when discussing treatments and administering procedures.
- Be cautious if others are present when discussing medical issues with the patient, ask if it is acceptable with the patient to have others present.
- Avoid discussions about patients in elevators and cafeteria lines.
- Do not leave messages on answering machines regarding patient conditions or test results.

- Avoid paging patients using identifiable information, such as their condition, name of physician, or unit that could reveal their health issues.
- Avoid leaving a patient's medical file on your computer screen when you leave your desk. It is best to log off/tap and go when leaving a workstation. In public areas, point computer monitors so that visitors or people walking by cannot view information.
- Avoid taking PHI off-site unless absolutely necessary and if you must, you are responsible for securing the PHI.
- Do not place PHI in the trash. Always shred unneeded paper documents containing PHI and place unneeded medical images in the appropriate receptacles for shredding.

What If You See Information You Do Not Need?

There likely will be occasions when you will have access to confidential information that you don't need for your work. For example, if a patient is placed in an isolation room, you may become aware of why he or she is there, or may suspect you know why. You may see patient information posted on whiteboards in restricted areas where the public cannot see them. You must keep this information confidential. Do not use it in any way, and do not disclose it to anyone, including coworkers, other patients, patient visitors, or anyone else who may ask.

Protecting Paper Records and X-Rays

When patient information is in your possession, regardless of form, you are responsible for keeping it safeguarded. Do not leave it unattended in an area where others can see it. This is especially important in public buildings, provider locations, and areas with heavy pedestrian traffic.

When you are done using patient information, either paper or film, return it to its appropriate location, e.g., the medical records department or a file at a nursing station.

When discarding paper patient information, make sure the information is shredded. X-Rays may be placed in confidential receptacles, located in all clinical areas of YNHH that are designated for the disposal of medical information (i.e., PHI). Leaving patient information intact in a wastebasket or box under your desk can lead to a privacy breach.

Security Considerations

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, breaches of privacy can be traced to lax security, so the two issues are intimately related. The HIPAA 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. If you will have access to Yale ePHI you must complete the online HIPAA Privacy and Security Training available at hipaa.yale.edu.

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. Connecticut medical records law requires that medical records be maintained for 7 years.

Business Associates

HIPAA defines business associates as entities outside of Yale that perform or assist Yale in performing activities that require the use or disclosure of PHI. The activities includes claims processing, data analysis, billing, practice management, or re-pricing.

Business associates also include lawyers, actuarial professionals, accountants, health care consultants, transcription agencies, computer support, data storage including cloud storage and billing companies. If you have a contract with someone helping you to do your job and it involves health information, he or she probably qualifies as a business associate.

Individuals at Yale cannot disclose protected health information to business associates unless the two parties have a contract. If you think you have a business associate relationship, contact your departmental business office or the HIPAA Privacy Office (hipaa@yale.edu).

Business associates are required to report any privacy breaches or security incidents to the Privacy Office. The Business Associate and Yale are obligated to take steps to mitigate the situation, which might include termination of the contract or reporting the business associate to the Secretary of the U.S. Department of Health and Human Services.

A good rule of thumb: Limit information provided to business associates to what's needed to do the job. If possible, provide de-identified data instead of patient-identifiable data.

Research

When is the Use of PHI in Research Permitted?

Research use of PHI is permitted under the Privacy Rule if any of the following conditions are met:

- Authorization is obtained from each individual in the study. This authorization is in addition to the normal informed consent process required under the Common Rule.

- An IRB approves a request for a waiver of authorization.
- All health information is de-identified.
- A "limited data set" (partially de-identified data) is used and a data use agreement is established with the organization providing the data.
- The data is used in a review preparatory to a research project, e.g., to develop a research protocol.
- The subjects are decedents.

The "Request for Access to PHI for Research Purposes" form indicates what supporting documentation or certifications are necessary to provide a research investigator with access to PHI. Requests for data, including lists of potential participants may be requested through the Joint Data Analytics Team (JDAT) at https://medicine.yale.edu/ycci/researchers/datarequests.aspx

Additional detailed guidance on the requirements of HIPAA in the context of research is available in the *Researcher's Guide to HIPAA* at www.hipaa.yale.edu.

HIPAA Contacts and Links

University HIPAA Privacy Office
2 Whitney Avenue, Suite 204
P.O. Box 208255
New Haven, CT 06520-8255
Phone: (203) 432-5919
Fax: (203) 432-4033
hipaa@yale.edu

Yale University HIPAA Web Site
includes both Privacy and Security Rule Information
http://hipaa.yale.edu/

U.S. Department of Health & Human Services, Office of Civil Rights, (OCR)
http://www.hhs.gov/ocr/hipaa/privacy.html

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

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 requires that all individuals in University HIPAA-covered components who handle protected health information in an electronic form (ePHI) or who use computing or communications systems during the course of their University work complete on-line training on the requirements of the Security Rule.

HIPAA Privacy and Security Training Certification

By signing below I certify that:

- ☐ I have read and understand the HIPAA Privacy for Clinicians Training and agree to the above HIPAA Privacy Training statements.

AND

- ☐ I do NOT provide treatment to Yale University, Yale Medicine, or Yale Health patients to whom I do not also provide treatment in my own non-University clinical practice and I do not have a Yale University email 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