Table of Contents

What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act which was passed into law by Congress in 1996. HIPAA includes requirements for ensuring that health information is kept private, establishes patient rights with regards to that information and creates standards for the protection of electronic health information.

HIPAA was designed with the goal of providing for increased access to health insurance and reducing health care costs by simplifying health insurance administration. The law in part promotes electronic transmission of standardized health insurance information. While this was expected to streamline health care administration, these large electronic data sets could also be misused. For example, computer databases can be used to easily identify individuals who have medical conditions which would require expensive care and that information could be used to hinder those patients' ability to obtain insurance coverage or employment. Public concern over privacy led Congress to include privacy and security requirements in HIPAA. These provisions were promulgated as the HIPAA Privacy Rule which went into effect April 14, 2003 and the HIPAA Security Rule that went into effect in April 2005.

Medical research institutions, health care organizations and health care providers have always voluntarily adopted and implemented professional practices to protect patient privacy. Under HIPAA, the obligation to ensure the privacy of patient information became federal law.

What is HITECH?

HITECH stands for the Health Information Technology for Economic and Clinical Health Act. HITECH included revisions to strengthen the HIPAA Privacy Rule, added breach notification and increased enforcement provisions. The changes included allowing patients to request electronic copies of their records, increasing accountability of business associates, and revising the authorization requirements for research uses. For a complete list of the changes see http://hipaa.yale.edu/resources/stay-current

Who needs to abide by HIPAA?

At Yale, all faculty, staff, trainees, students and others in or working in support of Yale's HIPAA Covered Components: the Schools 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, and Pharmacology) and Nursing, Yale Health, Department of Psychology clinics and the employee welfare benefit program (Benefits Office) are required to understand their responsibilities under HIPAA and adhere to Yale's HIPAA policies and procedures.

Are there penalties for not complying?

Protecting the privacy of health information is a major component of HIPAA. Civil and criminal penalties may be imposed by the Federal government for failure to comply with HIPAA, including up to a 10-year jail sentence and a fine of up to $1,500,000 per incident.

Within Yale we continuously monitor HIPAA compliance and follow up on concerns and complaints. In both cases, we may use audit reports of access to PHI contained in electronic systems, chart audits, site visits, interviews and file audits.

The privacy and security of Yale's health information are critical priorities of the University.

Employees who fail to follow HIPAA policies are subject to disciplinary action up to and including immediate termination of employment.

What is PHI?

PHI= Protected Health Information

PHI is the information that we must keep private under HIPAA.

PHI means any information that identifies an individual **and** relates to their health care including at least one of the following:

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

Note that patient names, in and of themselves, when derived from health care or payment for health care here are considered to be PHI and must be protected according to HIPAA.

What identifies an individual?

In addition to the obvious information such as the patient's name, Social Security number or medical record number, there are more obscure pieces of information that are considered identifiers under HIPAA such as date of birth, an internet protocol (IP) address, or the serial number on a medical device.

For a list of all identifiers see: http://hipaa.yale.edu/sites/default/files/files/5039-EX-De-ID-EXA.pdf

Whose records are covered by HIPAA?

HIPAA compliance covers the private health information of **EVERYONE.** Some of this information may relate to people you know: family members, coworkers, friends, acquaintances, members of clubs, churches or other organizations, neighbors, celebrities, etc. Remember HIPAA protection covers all of the private health information held in any form by 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, and Pharmacology), School of Nursing, Yale Health, Department of Psychology clinic, and the Benefits Office.

No one is left out!

Your job duties may lead you to come across information of people you know or you may have access to databases or files that would include people you know. If you do not need that information to do your job, you are violating HIPAA and Yale policy by looking at that information.

Note that some positions may require access beyond their immediate area in order to provide the best service to our patients. For example, an individual who schedules patient visits for one department may be asked by the patient to check upcoming visits to another department in the process of selecting an appropriate appointment time. Doing so is not absolutely necessary for scheduling the visit but is appropriate to maximize patient satisfaction and is allowable under HIPAA.

What if I am both a patient and an employee?

You may be both a staff member and a Yale patient. HIPAA policies do not prohibit you from accessing your own record. However, using your job related access to health information systems to access information of anyone else, including a person that you are legally authorized to represent such as your child, is not allowed unless you are doing so as part of your normal job functions. For example, if your role is to process payments and paperwork related to payment for services as part of your daily work, including services your child received, it is perfectly appropriate to process those claims.

What is meant by the "Minimum Necessary" Standard?

HIPAA requires that even after we limit access to those who need the information to perform their
job functions, we need to further limit access to what is the "**minimum necessary**" information. Minimum necessary refers to only accessing or disclosing those pieces of the PHI which are needed for a given activity.

Good clinical practice may require physicians to review the entire chart to provide care to a patient, making the entire record the "minimum necessary" information. On the other hand, when an internal auditor is reviewing claims made in relation to a research study, only those visits related to the research study in question constitute the "minimum necessary" information.

Depending on your job, you may handle charts often, but only need to actually read parts of it to obtain the necessary information. For example, when searching for notes or additional information that is needed or requested by a carrier to submit with a claim for reimbursement, additional payment, an appeal, etc., you would only need to go to the section of the chart that pertains to that information and search for the date(s) of service. The same criteria would apply when searching for notes using electronic software on your computer.

Reading through the documentation just to see a patient's medical history would not only be unnecessary and inappropriate, it would be in violation of HIPAA. When you need to see patient information to do your job, remember that the information is private and you are not allowed to repeat it, disclose it or share it with others unless they also need the information to do their job.

Your responsibility to maintain patient privacy continues even when you no longer work for Yale.

When can PHI be used within Yale without a signed patient authorization?

Under HIPAA guidelines, PHI can be accessed and used within Yale without a written patient authorization in limited ways such as:

- To provide treatment to that patient.
- To verify that patients are receiving quality care.
- To review and process benefit claims, including claims under the University's Flexible Benefits Plan.
- To fulfill administrative requirements such as physician credentialing, auditing, or legal review.
- To fulfill Yale's educational requirements to train students in medical care and administration.

In summary, PHI may be accessed for the purposes of **T**reatment, **P**ayment and health care **O**perations (TPO) without a signed written authorization from a patient.

For a complete list of when you can access PHI without a signed patient authorization, see HIPAA Policy 5031 at http://hipaa.yale.edu/policies-procedures-forms

When can PHI be disclosed to others outside of Yale without a signed patient authorization?

Under HIPAA guidelines, PHI collected by a healthcare organization or health plan can be disclosed to others who are not part of Yale without a signed patient authorization in limited circumstances. Some examples are:

- To the patient themselves or their legal representative.
- To physicians involved in the patient's care such as a physician who refers a patient to Yale or to whom Yale refers a patient.
- To the patient's insurance carrier to pay for treatment Yale provides except in cases where the patient has paid in full and requests that the information not be disclosed to their insurer.
- To organizations acting on Yale's behalf when an appropriate signed agreement known as a Business Associate Agreement is in place.
- To researchers if they have obtained a waiver of authorization from the IRB (Human Investigation Committee or Human Subjects Committee).
- To report certain communicable diseases to public health agencies.
- To appropriate government authorities regarding victims of abuse, neglect or domestic violence.
- To workers' compensation carriers for reporting and billing purposes.
- To medical examiners and funeral directors on behalf of deceased patients.
- To facilitate the donation and transplantation of organs.

For a complete listing of when PHI can be disclosed see HIPAA Policy 5031 at http://hipaa.yale.edu/policies-procedures-forms

Who do I go to with questions or complaints?

HIPAA requires each organization to appoint a Privacy Officer to oversee privacy practices under HIPAA. At Yale, this person is one of the key staff members responsible for developing the organization's privacy policies, monitoring and enforcing compliance with the law and responding to questions and complaints.

Deputy Privacy Officers at Yale School of Medicine, Yale School of Nursing, Yale Health, the Department of Psychology, and the Benefits Office are available to respond to day-to-day privacy matters.

When you have questions about privacy policies and the protection of individual patient health information, consult Yale's HIPAA web site (http://hipaa.yale.edu) which provides access to Yale's policies, procedures and guidance relating to HIPAA.

You can reach the Privacy Office at hipaa@yale.edu or by phone at 432-5919.

Patient complaints of privacy violations should be addressed through the standard patient complaint procedures of the clinical unit. They may also be addressed to the University Privacy Officer or the appropriate Deputy Privacy Officers.

Staff members who know or have reason to believe that someone has violated Yale's policies regarding HIPAA should report the matter promptly to their supervisor or a Privacy Officer. Anyone who expresses concern in good faith is protected by federal law against retaliation and harassment as a result of raising the concern. If there are concerns about possible retaliation or harassment they should be reported to the University Privacy Officer for further investigation and resolution.

If you have questions about the security of electronic PHI, you should contact Information Security at information.security@yale.edu.

How do I guard records?

Patient records should be stored so that:

- access is limited to those who need the records for legitimate purposes.
- paper files and films are stored in locked cabinets or in rooms that can be locked when staff is not around.

- electronic records are secure according to the requirements described in the HIPAA Security Rule.

For complete information about guarding electronic records go to the HIPAA Security Rule website at: http://www.hipaa.yale.edu/security.

Do not dispose of any type of records containing PHI in open receptacles or regular trash containers. Paper records that are no longer needed must always be shredded or placed in designated closed shredding receptacles. Contact your supervisor if the receptacle is full and a replacement is needed.

Access to computers and databases containing PHI must be limited through good password protection.

Never leave a disk, flash drive or anything containing patient information unattended in an in-box, or on a desk chair in an unlocked area. Deliver materials and documents that contain PHI personally to ensure privacy and unnecessary disclosure.

Laptops and other portable computing devices are particularly susceptible to loss or theft and are required to be encrypted using University endorsed encryption software. Follow the guidance on both the HIPAA Privacy and HIPAA Security web sites.

Store all computer disks and flash drives in locked areas and avoid labels that draw attention to the file content. Computers and external storage media must be fully erased prior to being discarded or re-used. Fully removing data requires more than just deleting files from the computer. See http://its.yale.edu/secure-computing/protecting-yales-data/secure-removal-data-or-disposal-computing-devices for more information.

How do I protect faxes?

Faxed patient information can easily fall into the wrong hands, which would be a violation of privacy and possible be considered a breach requiring notification to the patient and the US Department of Health and Human Services.

Check that the correct number is dialed into the fax or program frequently used numbers.

If you receive a fax in error, contact the sender and shred the information.

If you send a fax to the wrong number, contact the recipient and request that the fax be securely destroyed and then contact the Privacy Office to report the unauthorized disclosure.

Do not let faxed patient information lie around a fax machine unattended. Immediately place the faxed information in a secure and private location.

Be sure to always use a fax cover sheet that includes the HIPAA confidentiality statement.

Here is an appropriate HIPAA fax **Confidentiality Statement** that must be included on all faxes:

> The documents accompanying this transmission may contain confidential information that is legally protected. This information is intended only for the use of the individual or entity named above. **If you are not the intended recipient**, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately by calling us or sending a return fax indicating that you have arranged for the return or performed destruction of these documents.

How do I protect e-mail?

Sending PHI via e-mail to non-Yale, non-YNHH addresses is strongly discouraged because of privacy concerns:

- The message usually travels on the Internet and is not secure from unauthorized access while in transit.
- Emails are easily misdirected to the wrong recipient or to a recipient whose identity can not easily be verified.

If you must send PHI via email outside of the yale.edu, ynhh.org, bpth.org, or Greenwichhospital.org domains, you must adhere to the guidelines at http://hipaa.yale.edu/faq/guidance-faq/guidance-use-email-containing-phi including use of email encryption, Yale managed device, limiting identifiers and sensitive information to an absolute minimum and include the e-mail Confidentiality Notice.

Here is the HIPAA **e-mail Confidentiality Notice** that must be included on all e-mail containing PHI:

Please be aware that e-mail communication can be intercepted in transmission or misdirected. Please consider communicating any sensitive information by telephone, fax, or mail. The information contained in this message may be privileged and confidential. If you are NOT the intended recipient, please notify the sender immediately with a copy to hipaa.security@yale.edu and destroy this message.

Are there requirements for passwords and computer security?

Passwords and other security features that control access to computer systems help to protect PHI. They also make it possible for Yale to monitor who gains access to health records to ensure that they are being used appropriately.

The following procedures help to prevent the misuse of passwords:

- Never share passwords, never let someone else use your password, and never log into the system using borrowed credentials (a password or any other authorization method).
- Choose a password to make it as difficult as possible for someone to make educated guesses about what you've chosen.
- Try to choose a password that you will remember and don't have to write down.
- If you do write your password down, keep it in a secure and private location. Do not post your password or keep it where others can easily find it.

Employees who use computerized records must not leave their computers logged in to the patient information system while they are not at their workstations. When not in use, computer screens containing patient information or access to patient information must be turned away from the view of the public or people passing by.

You can lock your computer screen whenever you leave your computer unattended or out of your view – simultaneously press the Ctrl, ALT, Delete keys and then chose "Lock Computer" tab. You will need to sign on with your password to gain access when you return.

For complete information on HIPAA Security refer to: http://hipaa.yale.edu/security

What are Some Quick Tips for Protecting Patient Privacy?

- Use good judgment in oral communications and avoid unnecessary discussions, sharing and gossiping about patient information.
- Conduct any discussions with patients, or about patients, regarding their financial or health information in a private area and keep the information confidential.
- Do not discuss or share any patient's financial or health information with anyone who does not need the information to do their job.
- Never access or disclose patient information for personal reasons or out of curiosity.
- Be aware of your voice level when discussing patient information either on the phone or in person.
- If you need to discuss patient information with a coworker to do your jobs, do so face to face in an appropriate place. Avoid "over the cube," elevator or curb-side discussions.
- Be aware that you may not know who is on the other side of the cube.

- Be aware of individuals who come into your work area.
- Do not leave patient medical records where others can easily see or access them.
- Turn pages containing patient information over so PHI is face down.
- Keep laboratory, radiology, and other ancillary test results private.
- Arrange your work area to avoid public or unauthorized staff from viewing patient information.
- Do not leave screens containing patient information open on your computer.
- Do not leave your computer unattended – either log off or set your computer to automatically lock with password protection when unattended or manually lock your computer when you leave your computer area.
- Do not share your ID or passwords with anyone – you are responsible for activities tracked on a computer when your password is used.
- Always use a fax cover sheet with the HIPAA confidentiality statement – for both internal and external faxes.
- Verify fax numbers to which information is being sent.
- Program frequently used numbers into the fax machine.
- Do not leave documents on fax or copier machines.
- Should you receive a fax in error be sure to contact the sender and shred the information.
- Access, print, send, fax or e-mail only the "Minimum Necessary" information needed to do your job effectively.
- If applicable, lock cabinets or drawers containing PHI when not in use.
- Do not use the patient's name in the subject field of an e-mail.
- Double check e-mail addresses before hitting the send button.
- Never use your trash bin to discard documents containing patient information – always use Shred - it containers or shredders.
- Minimize the information listed on patient sign-in sheets to last names only if possible and change the sign in sheet twice a day.
- Be sure patient charts are protected from public view.