

HIPAAquick Training

HIPAA Introduction

HIPAA stands for Health Insurance Portability and Accountability Act of 1996. HIPAA is a federal law that defines much of how healthcare works today. HIPAA has requirements that entities like doctors, hospitals, and health plans have to follow. HIPAA also has requirements that we, as individual healthcare workers, have to follow as well.

HIPAA is a huge and complex law, many hundreds of pages long. But at its core, it is designed to do five things:

1. Make health insurance more portable – so workers and their families can more easily keep their health insurance coverage when they change jobs.
2. Reduce healthcare fraud and abuse – which normally wastes nearly one third of every healthcare dollar.
3. Improve efficiency and effectiveness – of payments and other transactions in healthcare.
4. Protect the privacy and security of medical records – so our confidential data is safe.
5. Build statistical data for analysis – so authorities and scientists better understand diseases and how they spread.

HIPAA affects nearly everything we do in healthcare, so it's vitally important to understand it. HIPAA includes serious fines, penalties, and sanctions if we carelessly or intentionally violate it. And yet HIPAA actually shields you from liability as long as you are careful, act in good faith, and meet HIPAA's basic legal requirements.

Important HIPAA Terms

Covered Entity – any doctor's office, clinic, hospital, nursing home, or other entity that is covered under HIPAA law. Covered Entities, also called CE's, have to meet certain conditions to be covered by HIPAA law, but for the most part, nearly every healthcare provider in America is a Covered Entity.

Protected Health Information (or PHI) – generally refers to patients' medical (and billing) records that are "protected" under HIPAA. PHI can be *any* individually identifiable information about a patient's health or condition, past, present, or future. PHI can be in any form: written, printed, recorded, photographed, or even spoken (oral). PHI may be either created or received by a Covered Entity. Either way, it is "protected" under HIPAA law from inappropriate uses or disclosures. When PHI must be permanently disposed of, it must be completely destroyed, preferably by cross-cut shredding or burning.

ePHI – This stands for "Electronic PHI". ePHI refers to any PHI that is in electronic form, such as on computers, copiers, faxes, and PDA's. ePHI is a part of HIPAA's Security Rule.

Minimum Necessary Rule – A HIPAA requirement that we must only use or disclose only the *bare minimum* PHI necessary to do a particular job or task. HIPAA says that we must make a "reasonable effort" to use, disclose, or request only the Minimum Necessary PHI in our daily work. One critical exception is for treatment purposes. For treatment, we do *not* have to limit PHI to the minimum necessary; physicians, nurses, and other caregivers may use every bit of PHI needed to treat patients.

Notice of Privacy Practices (or NPP) – A special printed Notice that HIPAA requires Covered Entities to give to their patients. The NPP tells patients briefly about how their PHI may be used or disclosed by the Covered Entity, and it also tells patients about their new HIPAA Rights and how to use them.

Business Associate (or BA) -- Any person or organization that's *not* part of a covered entity's workforce, who works for a covered entity and is exposed to PHI. Examples of Business Associates are medical laboratories and transcriptionists. Business associates are not covered directly under HIPAA law. However, they must sign special contracts with covered entities that hold them to similar legal standards as covered entities under HIPAA.

Parts of HIPAA

HIPAA has many different sections that covered entities have to be aware of. For us as individual healthcare workers, the two parts of HIPAA we need to understand most are the Privacy Rule and the Security Rule. These two parts of HIPAA are overlapping, complementary, and work together.

HIPAA's Privacy Rule – This is the portion of HIPAA that deals with protecting PHI in all its forms, including the medical charts and records most of us work with every day. The Privacy Rule sets standards all Covered Entities and their employees have to meet to protect patients' confidential medical records.

HIPAA's Security Rule – This part of HIPAA deals only with PHI in electronic form, called ePHI, that is used, stored, and transmitted by electronic devices and networks. Because ePHI can be easily erased, misplaced, or misdirected in a matter of seconds, HIPAA's Security Rule has special requirements to ensure the safety of ePHI.

HIPAA's Basic Requirements

All Covered Entities, regardless of size, as required under HIPAA to do certain basic things to be compliant with the law. Covered Entities are generally required to:

- ⇒ Provide information to patients about their privacy Rights and how their information may be used. This is done with the Notice of Privacy Practices, as a minimum.
- ⇒ Adopt clear Privacy and Security Policies & Procedures.
- ⇒ Train employees on (at least) the basics of HIPAA and the organization's own HIPAA Policies & Procedures.
- ⇒ Designating an individual (the HIPAA Privacy Officer and/or Security Officer) to be responsible for HIPAA compliance and for resolving patient complaints.
- ⇒ Secure patient records (with locked cabinets and doors) so they are protected from misuse or inappropriate disclosure.
- ⇒ Keep records of certain kinds of disclosures or releases of patients' PHI.
- ⇒ Retain most HIPAA compliance documents for a minimum of six years.
- ⇒ Adopt general physical safeguards to protect the facility and patient privacy and security.

Privacy Rule -- Disclosures

Disclosures of PHI are a daily fact of life for most of us in healthcare. And most of us learned early in our careers to be extra careful with what we disclose and who we disclose it to. HIPAA puts specific requirements and precautions in place to deal with disclosures. HIPAA recognizes fast, high-quality patient care as the top priority, and it balances the need to protect patient privacy with our need to use and disclose PHI. Before releasing PHI, HIPAA requires us to get *proof of identity* (such as a driver's license or other photo I.D.) in most cases.

Disclosures to Physicians and Caregivers – HIPAA allows us to both use and disclose a patient’s PHI without an authorization, as long as the use or disclosure is for treatment purposes. Thus, doctors and nurses may access complete medical records as needed for treatment purposes, *without* an authorization and without regard to the Minimum Necessary Rule. HIPAA also allows you to disclose all or part of a patient’s medical records to another doctor, such as a specialist or referral, without an authorization from the patient. The only requirement under HIPAA is that all the parties must have a treatment relationship with the patient, either in the past, presently, or in the future.

Disclosures to Patient’s Family and Friends – Despite what you may have heard, HIPAA *does* allow disclosures of PHI to the family and friends of a patient, with certain restrictions. First, the patient must be given the chance to agree or object to the disclosure, if he or she is conscious and of sound mind. If the patient objects, you should not disclose the PHI. If the patient cannot be asked, because of an emergency or because they are unconscious, HIPAA allows us to use “reasonable judgment” as to whether the disclosure is in the patient’s best interest. If your “reasonable judgment” tells you the disclosure is in the patient’s best interest, you may make the disclosure. If not, avoid making the disclosure. Finally, HIPAA says that we must apply the Minimum Necessary Rule in such disclosures, meaning that less is better than more in such cases.

Miscellaneous Disclosures – HIPAA permits a wide variety of other PHI disclosures, under certain conditions and with some restrictions. These include:

- ⇒ Disclosures for Law Enforcement Purposes – such as apprehending a criminal or fugitive.
- ⇒ Disclosures Required by Law – such as disease registries.
- ⇒ Disclosures for Workers Compensation – when these are necessary.
- ⇒ Disclosures in Emergency Situations – such as natural disasters, fires, civil unrest, etc.
- ⇒ Other Miscellaneous Disclosures – for national security or HIPAA enforcement.

Please see your HIPAA Privacy Officer for additional information about these miscellaneous disclosures. Also, your organization should have HIPAA Policies and Procedures in place to help guide employees in making or refusing such disclosures. Familiarize yourself with these.

Notice of Privacy Practices (NPP)

The Notice of Privacy Practices (NPP) tells patients how their PHI may be used or disclosed in your organization. The NPP also tells patients about their new HIPAA Rights and how to exercise those Rights. Finally, the NPP tells patients how to file a privacy-related complaint, either with your organization or with the federal government.

HIPAA law requires Covered Entities (CE’s) to give each patient a printed (or emailed) copy of the NPP at least once. The CE must make a good faith effort to get a signature from each patient, on a receipt or log sheet, which simply says that the patient received a copy. If the patient refuses to sign, that’s OK. An employee can sign and date the receipt or log, and write that the “patient refused”. The matter ends there. If the Covered Entity’s policies about uses and disclosures change substantially, a revised copy of the NPP must again be given to all patients. Otherwise, once is all that is required. Also, HIPAA requires that a copy of the NPP be “posted prominently” in the facility where patients can see it. Usually, this would be in a poster format on a wall, or in a book or binder in a waiting room.

Patients New HIPAA Rights – Described in the NPP are patients’ new Rights under HIPAA. Patients are guaranteed these new Rights, and we are required to help patients exercise their Rights. In most cases, there will be a simple form for the patient to fill out for each Right they wish to exercise. See your HIPAA Privacy Officer for the forms or for more details.

- ⇒ **Right to Receive a Notice of Privacy Practices** – This is a Right for the patient to receive a copy of the NPP, and a requirement for the Covered Entity to give a copy to each patient.
- ⇒ **Right to Copy & Inspect Own PHI** – This Right says that patients are entitled to get a copy of their medical records if they want, or to “inspect” (read through) their medical records if they wish, with certain conditions. A reasonable fee can be charged for copies of medical records. Fee amounts are usually set by individual states, not by HIPAA.
- ⇒ **Right to Request PHI Amendments** – This is a Right to request that an amendment (written note) be added to a patient’s own medical record. The Covered Entity does not have to agree to the request, but may if it is reasonable. Covered Entities may refuse if 1.) the data is correct; or, 2.) someone else originated the data in the record.
- ⇒ **Right to Restrict Disclosures to Others** – This Right allows a patient to name particular people they do *not* want to have access to any of their medical information. Covered Entities do not have to agree to such requests, but if they do, they must abide by the request consistently. Patients cannot restrict disclosures required by law.
- ⇒ **Right to Receive PHI by Alternate Means** – This Right allows patients to ask a Covered Entity to contact them at an alternate phone number or address. Examples might be where a patient asks that mail be sent only to their P.O. Box and not to their home; or, that any phone calls go only to the patient’s cell phone and not their home or work numbers.
- ⇒ **Right to Accounting of PHI Disclosures** – Under HIPAA, certain kinds of disclosures of a patient’s PHI must be recorded in a log. This Right allows patients to request a copy of the log showing these disclosures. Disclosures made for routine purposes (Treatment, Payment, and Healthcare Operations) *do not* have to be recorded in the log. For each recorded disclosure, the log shows the date, time, purpose, what was released, who received it, and who released it.
- ⇒ **Right to File a Privacy Complaint** – This Right says that a patient who believes that their privacy has been violated may file a complaint, in writing, with the Covered Entity where the problem occurred, or with the federal government. Retaliation against a patient for filing a complaint is not permitted. Complaints must be filed within 180 days of when the violation occurred. The Covered Entity must respond to the complaint within a reasonable time, and must attempt to reduce any harmful effects, if any, arising from the alleged violation. Note that *anyone* can file a complaint, not just patients.

Security Rule Basics

HIPAA’s Security Rule has numerous requirements to protect ePHI and the devices and networks that contain ePHI. Fortunately for most employees, nearly all of these must be implemented by management and technical people – not by most workers. For most of us, there are only a few basic guidelines we need to follow

For management, the Security Rule contains 36 separate “standards” that must be dealt with to be compliant. For the rest of us, here’s what we need to know:

- ⇒ Use strong passwords or pass-phrases and timer-based screen savers on all PC's. Screen savers should activate in no more than 2 minutes, and should require employees to log in again to use the computer.
- ⇒ Always use appropriate anti-virus and anti-spyware programs. Keep them updated regularly, if not automatically.
- ⇒ Never leave files and documents containing PHI open and unattended on computers. Close files and programs when you leave your workstation.

- ⇒ Never insert a diskette or CD in a work computer without thoroughly scanning it first. Always scan for viruses, spyware, and other threats before installing new data or programs. If you can't scan it, don't install or use it.
- ⇒ Use encryption for email containing PHI. If you are not set up to encrypt (and decrypt) email messages, don't include PHI in them.
- ⇒ Always securely delete ePHI. This should be done with file-wiping or file-shredding software. The windows "delete" function is not secure and does not really delete files.
- ⇒ Always follow your organization's Security Policies and Procedures, and immediately report problems or security breaches to your supervisor or HIPAA Security Officer.

HIPAA and Emergencies

Despite its strong stand on privacy and security, HIPAA law recognizes patient safety and care as the highest priorities. During an emergency, whether an individual emergency or a natural disaster, HIPAA specifically permits us to put patient care and safety first, and HIPAA last, if we are faced with such a choice. During an emergency, do your best to continue to protect PHI and ePHI. But if push comes to shove, remember: patient safety and care come first!

HIPAA Penalties & Sanctions

HIPAA law distinguishes between unintentional violations, such as simple non-compliance, and intentional violations that are done with malice or for personal gain. Unintentional violations are civil matters, and carry less severe penalties. Intentional violations are criminal matters and carry very severe penalties. Only Covered Entities and their employees can face HIPAA sanctions and penalties.

HIPAA carries civil and criminal penalties ranging from \$100 for simple, unintentional violations, to a maximum of \$250,000 and 10-year imprisonment for disclosure of PHI done with malicious harm or intent. Penalties can also include loss of accreditations, loss of medical licenses, and other sanctions.

Violations of HIPAA law are investigated by a division of the US Department of Health and Human Services (HHS) called the Office for Civil Rights, or OCR. There are ten regional OCR offices around the country, and each one handles privacy complaints and investigations for a specific set of states. If a violation is serious enough, it is referred to the US Department of Justice as a criminal investigation.

HIPAA General Safeguards & Advice

There are a number of simple things we can all do to remain compliant with HIPAA and avoid HIPAA-related problems:

1. Turn computer screens so that passers-by cannot see PHI on the screens. Alternately, use screen filters that block viewing from side angles.
2. When discussing PHI with anyone, lower your voice, or move to a quiet area if possible, to avoid being overheard.
3. Don't leave PHI out on desks, workstations, or counter tops where just anyone might be able to see it.
4. Always verify fax and phone numbers before sending or calling with PHI. If faxing, verify that the information was received by the right party. Use a strongly worded cover sheet for faxes.
5. Check credentials and verify people's identities before handing over any PHI or other critical information.

6. If accidental disclosures do happen, document them briefly, then sign and date the document. Notify your HIPAA Privacy Officer, and save such reports in case they are needed later.
7. If you are transporting medical records in your car, keep the records out of sight in the trunk, if possible, and always lock the vehicle securely.
8. Don't discuss patients, their treatment, or their PHI outside of work. You never know who may be listening.
9. Study and learn your organization's HIPAA Policies and Procedures. They are your best HIPAA guidance.
10. If you have questions about anything related to HIPAA, ask your HIPAA Privacy or Security Officer.

HIPAA Guidelines to Save and Remember

The two charts below are designed to help you remember the basics of HIPAA. Keep these handy at your desk or workstation, or in your office, as an easy reminder of how to avoid HIPAA problems and be safe with HIPAA. Please save your copy of this HIPAAquick Training Program for reference also.

Ten Points of HIPAA Privacy

1. **Protect PHI at all costs – your job and reputation depend upon it.**
2. **Access, use, or provide only the Minimum Necessary PHI to accomplish the task.**
3. **Cover, turn over, or lock pp PHI that is not immediately in use.**
4. **Report accidental or willful disclosures of PHI to your HIPAA Privacy Officer or Supervisor.**
5. **Do not discuss PHI outside of the work environment under any circumstances.**
6. **In emergencies, put patient care ahead of all else – even HIPAA.**
7. **Always dispose of PHI according to current Policies and Procedures.**
8. **When you must discuss PHI, lower your voice or move to a private area.**
9. **Protect PHI on computers, cellphones, fax machines, and other devices.**
10. **If in doubt about what to do, ask your Supervisor or HIPAA Privacy Officer.**

© Copyright 2009 HIPAA Group, Inc.
All Rights Reserved – No Unauthorized Duplication

Ten Secrets of HIPAA Security

1. **Protect ePHI at all costs – your job and reputation depend on it.**
2. **Identify the types of data subject to HIPAA rules: PHI and ePHI.**
3. **Use strong pass-phrases and timer-based screen savers on all PC's.**
4. **Never leave open files and documents containing ePHI unattended.**
5. **Always scan for viruses, spyware, and other threats before installing new data or programs.**
6. **Always use encryption for email containing ePHI. Don't use email for PHI without it.**
7. **Always file, shred, secure, or otherwise properly dispose of ePHI.**
8. **Protect ePHI on computers, cellphones, PDA's, fax machines, portable storage media, etc.**
9. **Immediately report security violations to your Supervisor.**
10. **If in doubt about what to do, ask your Supervisor or HIPAA Security Officer.**

© Copyright 2009 HIPAA Group, Inc.
All Rights Reserved – No Unauthorized Duplication

END HIPAAquick Training

Training Quiz A

1.) In HIPAA, the term “PHI” stands for:

- A. “Personal Health Information”
- B. “Protected Health Information”
- C. “Provider Health Information”

2.) HIPAA allows the use or disclosure of PHI without an Authorization for:

- A. Treatment purposes
- B. Payment purposes
- C. Healthcare Operations
- D. All of the above

3.) HIPAA penalties and sanctions apply only to:

- A. Healthcare “covered entities”, as defined by HIPAA
- B. Anyone who delivers healthcare services
- C. Healthcare “covered entities” and their non-healthcare business partners
- D. Doctors, nurses, and patients

4.) Under HIPAA, business affiliates who are paid for work involving PHI are called:

- A. “Business Associates”
- B. “Business Partners”
- C. “Vendor Partners”

5.) HIPAA penalties and sanctions can include:

- A. Monetary fines
- B. Loss of licensure and accreditation
- C. Jail time for willful, criminal offenses
- D. All of the above

6.) HIPAA allows sharing basic patient information with family & friends:

- A. As long as other basic HIPAA compliance requirements are met
- B. Even if the patient is comatose or unavailable because of emergency
- C. As long as the patient, if available and competent, does not object
- D. All of the above

7.) A simple way to protect PHI during conversations is to:

- A. Keep your voice low so your conversation can’t easily be heard
- B. Move the conversation to a more private area, if one is available
- C. Be aware of others around you who could overhear, and act accordingly
- D. All of the above

8.) When “PHI” needs to be permanently disposed of, it should be:

- A. Thrown in a trash bin or dumpster
- B. Returned to the patient or patients that the records are about
- C. Completely destroyed, preferably by cross-cut shredding or burning

9.) In a medical emergency, HIPAA allows you to:

- A. Disregard HIPAA temporarily and put patient safety above all else
- B. Cancel a patient’s medical bills
- C. Destroy a patient’s medical records

10.) For treatment purposes, HIPAA allows the unlimited use of all a patient’s PHI without an authorization:

- A. True
- B. False