Health Insurance Portability and Accountability Act

The following document is broken down into three parts

1. Your Rights under HIPAA
2. Appendix and Handouts
3. How Employees can help prevent HIPAA Violations

Your Rights under HIPAA

Retrieved from https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

HIPAA General Fact Sheets (See Appendix)

- Your Health Information Privacy Rights - PDF
- Privacy, Security, and Electronic Health Records - PDF
- Sharing Health Information with Family Members and Friends - PDF

Who Must Follow These Laws

We call the entities that must follow the HIPAA regulations "covered entities."
Covered entities include:

- **Health Plans**, including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.
- **Most Health Care Providers**—those that conduct certain business electronically, such as electronically billing your health insurance—including most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.
- **Health Care Clearinghouses**—entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

In addition, business associates of covered entities must follow parts of the HIPAA regulations.

Often, contractors, subcontractors, and other outside persons and companies that are not employees of a covered entity will need to have access to your health information when providing services to the covered entity. We call these entities "business associates." Examples of business associates include:

- Companies that help your doctors get paid for providing health care, including billing companies and companies that process your health care claims
- Companies that help administer health plans
- People like outside lawyers, accountants, and IT specialists
- Companies that store or destroy medical records

Covered entities must have contracts in place with their business associates, ensuring that they use and disclose your health information properly and safeguard it appropriately. Business associates must also have similar contracts with subcontractors. Business associates (including subcontractors) must follow the use and disclosure provisions of their contracts and the Privacy Rule, and the safeguard requirements of the Security Rule.

Who Is Not Required to Follow These Laws

Many organizations that have health information about you do not have to follow these laws.
Examples of organizations that do not have to follow the Privacy and Security Rules include:

- Life insurers
- Employers
- Workers compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices

What Information Is Protected

- Information your doctors, nurses, and other health care providers put in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer's computer system
- Billing information about you at your clinic
- Most other health information about you held by those who must follow these laws
  How This Information Is Protected
- Covered entities must put in place safeguards to protect your health information and ensure they do not use or disclose your health information improperly.
- Covered entities must reasonably limit uses and disclosures to the minimum necessary to accomplish their intended purpose.
- Covered entities must have procedures in place to limit who can view and access your health information as well as implement training programs for employees about how to protect your health information.
- Business associates also must put in place safeguards to protect your health information and ensure they do not use or disclose your health information improperly.

What Rights Does the Privacy Rule Give Me over My Health Information?
Health insurers and providers who are covered entities must comply with your right to:

- Ask to see and get a copy of your health records
- Have corrections added to your health information
- Receive a notice that tells you how your health information may be used and shared
- Decide if you want to give your permission before your health information can be used or shared for certain purposes, such as for marketing
- Get a report on when and why your health information was shared for certain purposes
- If you believe your rights are being denied or your health information isn't being protected, you can
  - File a complaint with your provider or health insurer
  - File a complaint with HHS

You should get to know these important rights, which help you protect your health information.
You can ask your provider or health insurer questions about your rights. (For more information, see Appendix)

Who Can Look at and Receive Your Health Information
The Privacy Rule sets rules and limits on who can look at and receive your health information
To make sure that your health information is protected in a way that does not interfere with your health care, your information can be used and shared:

- For your treatment and care coordination
- To pay doctors and hospitals for your health care and to help run their businesses
- With your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object
- To make sure doctors give good care and nursing homes are clean and safe
- To protect the public's health, such as by reporting when the flu is in your area
- To make required reports to the police, such as reporting gunshot wounds

Your health information cannot be used or shared without your written permission unless this law allows it. For example, without your authorization, your provider generally cannot:

- Give your information to your employer
- Use or share your information for marketing or advertising purposes or sell your information

Below you will find handouts for individuals retrieved from https://www.hhs.gov/hipaa/for-individuals/index.html

OFFICE FOR CIVIL RIGHTS

YOUR HEALTH INFORMATION PRIVACY RIGHTS

Most of us feel that our health information is private and should be protected. That is why there is a federal law that sets rules for health care providers and health insurance companies about who can look at and receive our health information. This law, called the Health Insurance Portability and Accountability Act of 1996 (HIPAA), gives you rights over your health information, including the right to get a copy of your information, make sure it is correct, and know who has seen it.

Get It.

You can ask to see or get a copy of your medical record and other health information. If you want a copy, you may have to put your request in writing and pay for the cost of copying and mailing. In most cases, your copies must be given to you within 30 days.

Check It.

You can ask to change any wrong information in your file or add information to your file if you think something is missing or incomplete. For example, if you and your hospital agree that your file has the wrong result for a test, the hospital must change it. Even if the hospital believes the test result is correct, you still have the right to have your disagreement noted in your file. In most cases, the file should be updated within 60 days.

Know Who Has Seen It.

By law, your health information can be used and shared for specific reasons not directly related to your care, like making sure doctors give good care, making sure nursing homes are clean and safe, reporting when the flu is in your area, or reporting as required by state or federal law. In many of these cases, you can find out who has seen your health information. You can:

- **Learn how your health information is used and shared by your doctor or health insurer.** Generally, your health information cannot be used for purposes not directly related to your care without your permission. For example, your doctor cannot give it to your employer, or share it for things like marketing and advertising, without your written authorization. You probably received a notice telling you how your health information may be used on your first visit to a new health care provider or when you got new health insurance, but you can ask for another copy anytime.
- **Let your providers or health insurance companies know if there is information you do not want to share.** You can ask that your health information not be shared with certain people, groups, or companies. If you go to a clinic, for example, you can ask the doctor not to share your medical records with other doctors or nurses at the clinic. You can ask for other kinds of restrictions, but they do not always have to agree to do what you ask, particularly if it could affect your care. Finally, you can also ask your health care provider or pharmacy not to tell your health insurance company about care you receive or drugs you take, if you pay for the care or drugs in full and the provider or pharmacy does not need to get paid by your insurance company.

- **Ask to be reached somewhere other than home.** You can make reasonable requests to be contacted at different places or in a different way. For example, you can ask to have a nurse call you at your office instead of your home or to send mail to you in an envelope instead of on a postcard.

If you think your rights are being denied or your health information is not being protected, you have the right to file a complaint with your provider, health insurer, or the U.S. Department of Health and Human Services.

To learn more, visit **www.hhs.gov/ocr/privacy/**.

For more information, visit **www.hhs.gov/ocr**.

U.S. Department of Health & Human Services
Office for Civil Rights

OFFICE FOR CIVIL RIGHTS

PRIVACY, SECURITY, AND ELECTRONIC HEALTH RECORDS

Your health care provider may be moving from paper records to electronic health records (EHRs) or may be using EHRs already. EHRs allow providers to use information more effectively to improve the quality and efficiency of your care, but EHRs will not change the privacy protections or security safeguards that apply to your health information.

EHRs and Your Health Information

EHRs are electronic versions of the paper charts in your doctor's or other health care provider's office. An EHR may include your medical history, notes, and other information about your health including your symptoms, diagnoses, medications, lab results, vital signs, immunizations, and reports from diagnostic tests such as x-rays.

Providers are working with other doctors, hospitals, and health plans to find ways to share that information. The information in EHRs can be shared with other organizations involved in your care if the computer systems are set up to talk to each other. Information in these records should only be shared for purposes authorized by law or by you.

You have privacy rights whether your information is stored as a paper record or stored in an electronic form. The same federal laws that already protect your health information also apply to information in EHRs.

Benefits of Having EHRs

Whether your health care provider is just beginning to switch from paper records to EHRs or is already using EHRs within the office, you will likely experience one or more of the following benefits:

- **Improved Quality of Care.** As your doctors begin to use EHRs and set up ways to securely share your health information with other providers, it will make it easier for everyone to work together to make sure you are getting the care you need. For example:
  - Information about your medications will be available in EHRs so that health care providers don't give you another medicine that might be harmful to you.
  - EHR systems are backed up like most computer systems, so if you are in an area affected by a disaster, like a hurricane, your health information can be retrieved.
  - EHRs can be available in an emergency. If you are in an accident and are unable to explain your health history, a hospital that has a system may be able to talk to your doctor's system. The hospital will get information about your medications, health issues, and tests, so decisions about your emergency care are faster and more informed.

- **More Efficient Care.** Doctors using EHRs may find it easier or faster to track your lab results and share progress with you. If your doctors' systems can share information, one doctor can see test results from another doctor, so the test doesn't always have to be repeated. Especially with x-rays and certain lab tests, this means you are at less risk from radiation and other side effects. When tests are not repeated unnecessarily, it also means you pay less for your health care in copayments and deductibles.
- **More Convenient Care.** EHRs can alert providers to contact you when it is time for certain screening tests. When doctors, pharmacies, labs, and other members of your health care team are able to share information, you may no longer have to fill out all the same forms over and over again, wait for paper records to be passed from one doctor to the other, or carry those records yourself.

Keeping Your Electronic Health Information Secure

Most of us feel that our health information is private and should be protected. The federal government put in place the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule to ensure you have rights over your own health information, no matter what form it is in. The government also created the HIPAA Security Rule to require specific protections to safeguard your electronic health information. A few possible measures that can be built in to EHR systems may include:

- "Access control" tools like passwords and PIN numbers, to help limit access to your information to authorized individuals.
- "Encrypting" your stored information. That means your health information cannot be read or understood except by those using a system that can "decrypt" it with a "key."
- An "audit trail" feature, which records who accessed your information, what changes were made and when.

Finally, federal law requires doctors, hospitals, and other health care providers to notify you of a "breach." The law also requires the health care provider to notify the Secretary of Health and Human Services. If a breach affects more than 500 residents of a state or jurisdiction, the health care provider must also notify prominent media outlets serving the state or jurisdiction. This requirement helps patients know if something has gone wrong with the protection of their information and helps keep providers accountable for EHR protection.

To learn more, visit **www.hhs.gov/ocr/privacy/**.

For more information, visit **www.hhs.gov/ocr**.

U.S. Department of Health & Human Services
Office for Civil Rights

OFFICE FOR CIVIL RIGHTS

SHARING HEALTH INFORMATION WITH FAMILY MEMBERS AND FRIENDS

There is a federal law, called the Health Insurance Portability and Accountability Act of 1996 (HIPAA), that sets rules for health care providers and health plans about who can look at and receive your health information, including those closest to you – your family members and friends. The HIPAA Privacy Rule ensures that you have rights over your health information, including the right to get your information, make sure it's correct, and know who has seen it.

What Happens if You Want to Share Health Information with a Family Member or a Friend?

HIPAA requires most doctors, nurses, hospitals, nursing homes, and other health care providers to protect the privacy of your health information. However, if you don't object, a health care provider or health plan may share relevant information with family members or friends involved in your health care or payment for your health care in certain circumstances.

When Your Health Information Can be Shared

- Under HIPAA, your health care provider may share your information face-to-face, over the phone, or in writing. A health care provider or health plan may share relevant information if:
- You give your provider or plan permission to share the information.
- You are present and do not object to sharing the information.
- You are not present, and the provider determines based on professional judgment that it's in your best interest.

Examples:

- An emergency room doctor may discuss your treatment in front of your friend when you ask your friend to come into the treatment room.
- Your hospital may discuss your bill with your daughter who is with you and has a question about the charges, if you do not object.
- Your doctor may discuss the drugs you need to take with your health aide who has come with you to your appointment.
- Your nurse may **not** discuss your condition with your brother if you tell her not to.
- HIPAA also allows health care providers to give prescription drugs, medical supplies, x-rays, and other health care items to a family member, friend, or other person you send to pick them up.

A health care provider or health plan may also share relevant information if you are not around or cannot give permission when a health care provider or plan representative believes, based on professional judgment, that sharing the information is in your best interest.

Examples:

- You had emergency surgery and are still unconscious. Your surgeon may tell your spouse about your condition, either in person or by phone, while you are unconscious.
- Your doctor may discuss your drugs with your caregiver who calls your doctor with a question about the right dosage.
- A doctor may **not** tell your friend about a past medical problem that is unrelated to your current condition.

For more information about sharing your health information with family members and friends, or more information about HIPAA, visit **www.hhs.gov/ocr/privacy/hipaa/understanding/index.html**.

For more information, visit **www.hhs.gov/ocr**.

U.S. Department of Health & Human Services
Office for Civil Rights

How employees can prevent HIPAA violations

10/3/2017 – Retrieved and adapted from https://www.hipaajournal.com/employees-prevent-hipaa-violations/

Listed below are some of the common ways HIPAA Rules are violated by employees.

Never Disclose Passwords or Share Login Credentials

Every employee is provided with a unique login, through which they will be granted access to sensitive information. It is therefore essential that those login details remain private. Login credentials should never be shared or written down. Login information is used to track the actions of users, including activities involving ePHI. If another employee has your login credentials, and improperly accesses ePHI using those credentials, it will be your job that is on the line.

Never Leave Portable Devices or Documents Unattended

The Office for Civil Rights breach portal is littered with reports of data breaches involving lost and stolen devices and mishandled PHI. A lost or stolen device containing ePHI is reportable under HIPAA Rules if the device is not encrypted. The Office for Civil Rights investigates reports of lost and stolen devices to determine if HIPAA Rules have been violated. If those devices are discovered to have been left unattended, financial penalties may be issued. Portable devices must never be left unattended and when in use.

The same applies to paper records. Even when busy, healthcare employees must never leave documents containing PHI in areas where they can be viewed by unauthorized individuals, picked up by other healthcare workers, or seen by other patients.

You can prevent HIPAA violations by reminding employees who are not taking sufficient care with patient files about the risk of accidental disclosures of PHI.

Do Not Text Patient Information

Text messages are a quick and easy way to communicate, whether via the SMS network, WhatsApp, or Facebook Messenger. Unfortunately, none of the common messaging services have the necessary controls to prevent accidental disclosures of ePHI to unauthorized individuals.

For example, SMS messages are not encrypted and can easily be intercepted. WhatsApp is encrypted, but lacks appropriate authentication controls. In order for a text messaging service to be used, your employer must have signed a HIPAA-compliant business associate agreement with the service provider. If you need to send ePHI, only do so through approved channels such as a secure, healthcare text messaging platform.

Don't Dispose of PHI with Regular Trash

While most healthcare organizations have now transitioned to electronic health records, documents are still widely used. Any document containing the PHI of a patient must be kept secure at all times and disposed of securely when no longer required. HIPAA requires all PHI to be rendered unreadable, indecipherable, and unable to be reconstructed when it is no longer needed. Your employer should have strict rules covering the disposal of PHI which prohibits the disposal of documents with regular trash. You must be extremely careful to ensure that any paper copies of PHI are disposed of securely.

Never Access Patient Records Out of Curiosity

The accessing of patient health records by employees, without any legitimate reason for doing so, is a serious violation of HIPAA Rules and patient privacy. While the majority of healthcare employees respect the privacy of patients, there have been numerous cases over the years of patients snooping on the records of patients.

Healthcare employees are only permitted to view patient records if they are required to do so for treatment, payment and healthcare operations. For treatment purposes, employees are only permitted to view the records of their own patients.

The HIPAA Security Rule requires covered entities to maintain access logs to ensure inappropriate ePHI access can be identified. Those logs must be regularly reviewed. Depending on the system in place, a flag could be immediately raised

or it may take until the next audit for the privacy violation to be discovered, but Improper accessing of PHI will be identified.
If medical records are accessed without authorization it is likely to result in termination, and potentially criminal penalties against the individual concerned. Such actions are also likely to make it difficult to obtain future employment at other healthcare organizations. Your employer can also face heavy fines and considerable reputation damage.

Don't Take Medical Records with You When You Change Job

When employees leave a practice, they can be tempted to take PHI with them. Some new employers may even encourage this – the information could be used to recruit patients or sell them medical services or equipment. However, taking medical records, even if there has been a longstanding relationship with the patient, is data theft and could result in criminal charges.

Don't Access Your Own Medical Records Using Your Login Credentials

The HIPAA Privacy Rule allows patients to obtain copies of their health records on request, but healthcare employees do not have the right to access their medical records using their login credentials. Typically, healthcare providers require staff to go through the same process as patients. In order to gain access to their health data, they must submit a request for a copy of their health information via their HIM department.

Do Not Share ePHI on Social Media (Including Photos)

Many healthcare organizations have developed policies covering the use of social media by their employees and clearly state that details of work activities should not be shared via social media accounts. The sending of a tweet containing personally identifiable information of a patient is a serious HIPAA violation. The same applies to posting on Facebook, even in a closed Facebook group. That includes ePHI and gossip about a patient.
PHI includes health information, but also photographs and videos. In such cases, it doesn't matter if the photograph does not include the patients name. Patients could easily be identified from the photograph.
Selfies taken at work and posted to social media accounts would violate HIPAA Rules if patients are included in the photograph if prior consent has not been obtained in writing. It would also be a HIPAA violation if PHI can be seen in the photographs – documents and charts etc. If in any doubt about HIPAA Rules, don't post on social media without speaking to your compliance officer. The National Council of State Boards of Nursing (NCSBN) has published a useful guide for nurses on the use of social media.
There have been several high-profile cases of nurses and other healthcare employees taking photographs or videos of patients and uploading them to social media accounts. Inappropriate sharing of PHI can attract significant financial penalties for the covered entity, termination of employment contracts, loss of licenses, and lawsuits.

Report Potential HIPAA Violations

If you believe a colleague has violated HIPAA Rules it is important to take action to prevent similar incidents from occurring in the future. Report potential HIPAA violations internally to your compliance officer so that action can be taken promptly to address the problem. If you believe your organization is not doing enough to prevent HIPAA violations, consult your compliance officer. If HIPAA Rules are being regularly violated, you can file a complaint with the HHS' Office for Civil Rights.

Other Considerations adapted from Joy Hicks

1. Routine Conversation. Avoid disclosing information through routine conversation. Attempt to avoid gossip
2. Public Areas. Avoid discussing patient information in waiting areas, hallways, elevators, or any area that may be overheard by visits and/d patients. Be sure to keep patient records out of areas that are accessible to the public.
3. Marketing. Selling patient lists or disclosing PHI to third parties for marketing purposes is strictly prohibited without prior authorization from the patient. Remember that disclosure of patient information should only be accessed for the purpose of providing quality care.