

The requirements of the HIPAA Privacy Rule and Security Rule govern every health care agency's privacy and security practices and dictate our commitment to protect the privacy and security of the health information of patients. It's important that as an employee of a home care agency, you understand your responsibility to help ensure that we all do everything possible to protect patient health information from unauthorized uses and disclosures.

So, who must comply with the HIPAA Privacy and Security Rules?

Covered entities include Health Care Providers, Health Plans, Health Care Clearinghouses and Medicare Prescription Drug Card Sponsors. Health Care Providers include any provider of medical or other health care services or supplies who transmits any health information in electronic form. An example of this is submitting claims to Medicare. Health Plans consists of any individual or group plan that provides or pays the cost of health care, for example, a health insurance company, Medicare and Medicaid and physicians. Health Care Clearinghouses covers a public or private entity that processes another entity's health care transactions, like providing billing services. Lastly, Medicare Prescription Drug Card Sponsors include a nongovernmental entity that offers an endorsed discount drug program under the Medicare Modernization Act.

What is HIPAA?

The Health Insurance Portability and Accountability Act, frequently referred to as HIPAA for short, is a Federal Law that was enacted in 1996. Prior to the enactment of this HIPAA law, each state had different policies for insuring that a patient's privacy was protected. HIPAA provides a uniform standard that all states must follow. The Administrative Simplification provisions of HIPAA significantly impacted health care providers. The three major components include the Transactions Rule, the Privacy Rule and the Security Rule.

HIPAA Transactions Rule

HIPAA Transactions Rule. The goal of the Transactions Rule is to simplify and standardize how certain electronic transactions are conducted. All health care providers, health plans, employers, and individuals are now required to use the same health care transactions, code sets and uniform set of identifiers to ensure that electronic transactions are standardized and protected. By doing this, the health care industry is more efficient, uses technology more effectively and hopefully reduces costs.

HIPAA Privacy Rule. The purpose of the Privacy Rule is to protect health information from unauthorized use or disclosure. It requires that health care agencies develop systems and processes to safeguard patients' health information. The Privacy Rule provides, for the first time, nationwide minimum standards for protecting the privacy of health information. Before the Privacy Rule was enacted, it was up to individual states to protect a patient's privacy. Some states did a good job, others didn't. With the Privacy Rule, all health care consumers throughout the United States have a similar level of privacy protection. Most importantly, the Privacy Rule enforces that consumers have more control over how their health information is used and disclosed.

The Privacy Rule is a Federal law and all covered entities are mandated to comply with it. It is not optional. Protecting patient privacy and ensuring that a patient's health information is safeguarded is the right thing to do. In order to meet these requirements, everyone who works for a home care agency must understand his or her responsibilities with respect to patient health information. Compliance with these regulations involves significant effort on everyone's part to protect every patient's health information. If covered entities do not comply with the requirements of the Privacy Rule, they risk facing significant civil or criminal penalties – in the worst case scenario, even jail. Home care agencies require that all their employees comply with their privacy practices. Failure to comply will result in disciplinary action, up to and including termination of employment.

What health information must be protected under this federally mandated Privacy Rule? If you guessed personally identifiable information and Protected Health Information, you are correct.

Personally Identifiable Information or PII, is defined as a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: social security number; driver's license number or state issued identification card number; or financial account number, insurance policy number, credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account, provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

Protected Health Information or PHI, is any information related to a patient's health condition that could identify the patient. This information, whether in electronic, written or oral form, may be maintained in medical records, in computers, in conversations we have with each other, in reports or in billing records – everywhere throughout the home care agency. It is our job to protect our patients' past, current and future health information from being used or disclosed in unauthorized ways and/or that violate their privacy.

There are many things that health care agencies do to comply with the requirements of the Privacy Rule. These include issuing a formal notice of privacy practices, designating privacy and security officers, and having Privacy and Security Policies and Procedures.

We have a Privacy Officer and a Security Officer at the VNA Care. These officers implement & provide oversight of our Patient Privacy and Security Policies and Procedures related to protection of health information and federal and state regulations pertaining to patient privacy and safety. Our Privacy Officer is responsible for all matters related to privacy in the agency and for ensuring that policies and procedures related to our privacy practices are followed. The privacy officer receives and follows up on any complaints related to privacy violations. If you have questions or concerns about patient privacy or to report any violations that you witness, contact our Privacy Officer or call the Compliance Hotline.

Our Security Officer is responsible for all matters related to the security of protected health information transmitted and/or maintained in any electronic format. This is accomplished by coordinating initial and subsequent information risk assessments and audits. The Security Officer also administers the process for receiving, investigating and taking action on incidents and complaints concerning any potential breach of the Network's Security Policies and Procedures. Any concerns should be addressed to our Security Officer.

When is it allowable to use or release PHI? The Privacy Rule explains three ways that a patient's health information is legally allowed or required to be used or disclosed. The three reasons are: treatment, payment and health care operations or when required by federal, state or local law. For all other disclosures, we must obtain a signed authorization form from the patient.

- **Treatment.** The definition under HIPAA is broader than its normal use. Treatment includes not only providing health care services, but also covers all health care providers that are coordinating and managing a patient's care. Some examples include discussions with referral centers, case conferences with therapists, supervision and coordination of home health aides and obtaining orders from physicians. None of these activities require a patient's authorization. We often receive calls from a clinician asking if he or she may discuss a patient's care with another provider that is involved with the patient. The answer is yes you may, since each party is involved in that patient's care.
- **Payment** refers to all matters related to obtaining or providing reimbursement for health care services provided to the patient.
- **Health care operations** include many of the day to day activities required to run an agency and support patient care. For example, PHI is allowed to be used or disclosed for such things as performance improvement activities, risk management, training and auditing patient records.

Complying with the Privacy Rule requires that the disclosure of information must be kept to the **minimum amount necessary**, specific safeguards must be in place for the protection of written, oral and electronic health care information, and patient privacy rights must be honored. What does the Privacy Rule mean when it says “**minimum necessary standard.**” We must limit the amount of PHI used by a staff member to the minimum amount necessary to perform his or her job effectively. You must be aware of the amount of PHI to which you are entitled access in order to perform your job.

Providing health services to home care and hospice patients and providing wellness services is what we do. We cannot care for patients without talking to them and about them. We are allowed to use and disclose PHI for treatment, payment and health care operations. We are not allowed to violate patient confidentiality. **Oral PHI** is found in conversations we have about patients; during patient-centered conferences and team meetings; when we talk on telephones or cell phones; and in phone messages at the office or left on answering machines.

Some ways to protect oral PHI include the following: do not talk about patients in public places or where non-authorized staff or people can overhear your conversation; do not talk about a patient to anyone not involved in the patient's care; and do not discuss other patients on the phone, i.e., with other staff or with a physician, while in another patient's home.

Next, let's look at the **specific safeguards that must be in place for the protection of written, oral and electronic health care information**. If we use or disclose PII or PHI in ways that are not allowed by the Privacy Rule, we not only violate a patient's privacy, but we are also subject to significant fines and penalties. It is everyone's responsibility to ensure that written, oral and electronic PII or PHI is safeguarded.

Because PII or PHI is so central to everything we do, it is present throughout the agency in written form. It can be found in file cabinets; medical records; reports; the paperwork that a clinician uses in the home in the provision of care; desks; trash or recycle bins; fax machines; printers; copiers; near shredders as well as in staff mailboxes.

It is necessary to protect PII or PHI in the following ways: field staff should lock all written materials with PII or PHI in your trunk when not using them; have only the minimum amount of PII or PHI needed in the paperwork that a clinician uses in the home in the provision of care; promptly shred PII or PHI that is no longer needed or discard in a bin for confidential documents; don't leave PII or PHI unattended on your desk or in your work area; lock file cabinets containing PII or PHI when not in use; and remove PII or PHI from photocopiers, fax machines and printers.

What is the HIPAA Security Rule? It became effective in April 2005 for all health care providers. Its requirements control how PHI, that same information we already safeguard under the HIPAA Privacy Rule, is protected when that information is in Electronic Systems. Under the Security Rule, PHI is referred to as Electronic Protected Health Information or ePHI, for short. Electronic PHI or PII, is particularly vulnerable to misuse, loss, destruction or accidental disclosure. Remember, this information is also regulated by the HIPAA Security Rule. The major difference is that the Security Rule sets mandated requirements for ePHI and ePII, whereas the Privacy Rule regulates all PII or PHI.

What is ePHI or ePII? It is all patient or personal information that is transmitted or stored using any electronic media, such as a computer hard drive; laptop computer; PDAs; e-mail; electronic billing claims; magnetic tape or discs; on CD-ROMS, diskettes and memory sticks; transmitted in faxes; on computer networks or intranets; and in transmissions over the internet.

The Security Rule protects confidentiality, where ePHI or ePII is accessible only by authorized people and processes. It ensures integrity, where ePHI or ePII is protected from accidental or intentional alteration, loss or destruction in an unauthorized manner. It also limits availability, where ePHI or ePII can only be accessed as needed by authorized persons.

All employees have electronic access according to their specific job functions, which is limited to what is necessary for their particular position. Some employees may not have access to patient information if their job functions do not require them to be involved with patient data. Each health care agency must determine who can access PHI and/or ePHI, as regulated by the Privacy & Security Rules.

We can only disclose or request from others the minimum amount of PHI or PII needed to achieve the purpose of the disclosure or request. Our agency's policies and procedures identify the minimum amount of PII, PHI, ePII, or ePHI necessary in each of these instances. They also determine those circumstances when use, disclosure or request of a patient's entire medical record is necessary.

Some ways to protect ePHI or ePII include the following: locate fax machines in secure areas; always use a fax coversheet that includes a confidentiality statement and instructions for misdirected faxes; do not leave computer screens with PII or PHI unattended; never share your computer password with others or use someone else's password. Do not give it to your manager or even an IS person. There are ways of sharing data without sharing this information. Just ask. You should never be asked for your password. Do not include PII or PHI in email transmissions unless authorized to do so; and make sure that PII or PHI on your computer or laptop is password protected.

Can ePHI or ePIL be sent over the internet? Although the following refers to ePHI, the same safeguards can be used for ePIL. The Security Rule allows for ePHI to be sent over an open network as long as it is adequately protected from others that do not have the right to view the ePHI. This is accomplished by using an encryption system to protect the information. Encryption, also referred to as encoding, converts data or information into code so it can only be read by the sender and the intended recipient.

Other security measures that have been instituted at the VNA Care include the implementation of an automatic computer lock after 30 minutes of inactivity on the desktop. This process will protect patient data from being accessed by others who do not have permission to view the ePHI or ePIL. Also, all computer users must sign a User Access Agreement prior to obtaining access to ePHI or ePIL. Access to ePHI or ePIL by employees who resign or temporary employees/consultants is promptly discontinued. Each computer user has a unique USER ID and every user must create a new password every 90 days to protect access to his or her computer.

How can you help to keep the **computer system free from malicious software/viruses**? To protect desktop and laptop computers from viruses, DO NOT add any software to your computer system. Another important practice is not to open any email attachment from someone you don't know. A desktop and laptop computer is for work purposes only. On-going audits are performed by the Information Systems Department to track potential problems. Do not click on links in emails. You will be notified by voicemail if emails requiring you to click on a link is sent out.

Now, let's look at another component of the Privacy Rule which mandates that patient privacy rights must be honored. **Under the Privacy Rule, each patient has the following seven rights.** All of these rights are explained in our agency's Notice of Privacy Practices. We need to be aware of the patient privacy rights and what a patient needs to do to exercise them. If a patient asks you a question about his or her rights and you are not sure of the answer, contact your supervisor or manager, or call the agency's Privacy or Security Officer to get the correct response.

7 Patient Rights

1. All patients have the right to be informed about how their health information is used and disclosed. The Notice of Privacy Practices provides this information and all patients have a right to receive a copy of it. Each clinician provides a copy of our Notice of Privacy Practices to every patient on service at the VNA Care during the initial home visit before care is provided to him or her. We are required to obtain a written acknowledgement from every patient that he or she has received a copy of our Notice of Privacy Practices. If we are unable to obtain the patient's written acknowledgement, we must document in the patient's medical record our efforts to do so and explain why we were not able to obtain it.
2. Patients or their representatives have the right to lodge complaints about our privacy practices. The process for lodging complaints is outlined in our Notice of Privacy Practices. The agency's Compliance Officer will follow up on every complaint received. Staff and volunteers may also make complaints to the Compliance Officer if they become aware of any potential

privacy violations. It is everyone's responsibility to protect patient privacy and make sure we are meeting the requirements of the law.

3. Notice of Privacy Practices details all the permitted and required uses and disclosures of a patient's health information. The patient may request restrictions on how PHI is used or disclosed, even though it is allowed by the Privacy Rule. There is a formal process that must be followed for patients to request restrictions and it is described in our agency's policies and procedures. Our agency notifies the patient in writing whether the request is accepted or denied and the reasons for the decision. Refer to our agency's policies for more information regarding this.
4. Patient may request that he or she be communicated with in a manner or at a location that may be different from how or where we would normally communicate with him or her. Whenever possible, we try to accommodate all reasonable requests. When a patient has requested confidential communications, all staff that provide care to the patient must be aware of the changes in communication with that patient.
5. Patient may request access to his or her health information in order to inspect or copy it. There are very specific procedures that must be followed to review and grant or deny requests for access. If your job involves entering information in the patient's clinical record, which is a legal document, remember that your documentation may be read by the patient. As always, it is imperative to ensure clear, concise and accurate documentation.
6. Patient may believe his or her medical records contain errors. If so, he or she may request to have the information corrected. There is a very specific procedure that must be followed to review and grant or deny requests for an amendment. All requests for an amendment are reviewed on a case-by-case basis, according to our agency's policies and procedures.
7. Patients may request an accounting of the disclosures of their health information. The accounting does not have to include disclosures made for treatment, payment, or health care operations. It also does not need to include disclosures that the patient has authorized. It is likely that accountings will mostly include disclosures made for public health purposes. Again, there are very specific request procedures that must be followed that are detailed in our agency's policies and procedures.