

HIPAA Compliance for Pharmacies Part One: HIPAA Rules and Best Practices

August 15, 2023

By Michael H. Cohen

Pharmacies across the country need to understand and comply with the Health Insurance Portability and Accountability Act of 1966. According to the [US Centers for Disease Control and Prevention](#) (CDC), HIPAA is a federal law that provides national standards to protect sensitive patient information from being disclosed without their knowledge or consent.

The US Department of Health and Human Services (HHS) issued a [Privacy Rule](#) and a [Security Rule](#) to implement the law's requirements and to specifically protect a subset of the information (electronic patient information) that the Privacy Rule covers. HHS also has an [Enforcement Rule](#) to ensure compliance with HIPAA.

The HIPAA Privacy Rule

The HIPAA Privacy Rule applies to the use and disclosure of "protected health information" (PHI) by "covered entities." The Privacy Rule also includes standards for how the PHI is used. The aim of the Privacy Rule is to ensure that there is a proper balance between protecting PHI and "allowing the flow of health information needed to provide and promote high-quality healthcare, and to protect the public's health and well-being.

FIVE STEPS TO MEET HIPAA OBLIGATIONS AND PRIVACY & SECURITY COMPLIANCE

If you're submitting claims electronically for reimbursement, you are under **HIPAA**. This subjects you to all the privacy and security obligations of **HIPAA**. Simply having an electronic medical record system that says, HIPAA Compliant, is not going to be enough.

The HIPAA Security Rule

The HIPAA Security Rule protects the confidentiality, integrity, and availability of electronic protected health information. Electronic refers to the subset of PHI that is digital.

Covered Entities

HIPAA's Privacy and Security Rules apply to "covered entities." Covered entities are defined as:

- **Healthcare providers.** *"Every healthcare provider, regardless of size of practice, who electronically transmits health information in connection with certain transactions. These transactions include:*
 - *Claims*

- *Benefit eligibility inquiries*
- *Referral authorization requests*
- *Other transactions for which HHS has established standards under the HIPAA Transactions Rule.”*
- **Health plans.** Health plans include:
 - Health, dental, vision, and prescription drug insurers
 - Health maintenance organizations (HMOs)
 - Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers
 - Long-term care insurers (excluding nursing home fixed-indemnity policies)
 - Employer-sponsored group health plans
 - Government- and church-sponsored health plans
 - Multi-employer health plans

An exception may apply for smaller self-administered employer plans

- **Healthcare clearinghouses.** These are defined as *“Entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, healthcare clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or healthcare provider as a business associate.”*

HIPAA also applies to “business associates” who are people and organizations (with some exceptions) who use the PHI for claims processing, data analysis, utilization review, and billing. Business associates may be directly liable for HIPAA violations. Pharmacies and other healthcare practices may be liable for any HIPAA violations of their business associates.

HIPAA compliance for pharmacies – The Rules

According to the HIPAA Journal (which provides numerous articles on HIPAA compliance, HIPAA certification, HIPAA software, and many other HIPAA-related topics), most pharmacies do need to comply with HIPAA’s Privacy and Security Rules and, possibly, other even more stringent requirements.

Pharmacy-related HIPAA topics include the following:

How Do Pharmacies Qualify Under HIPAA

While most pharmacies qualify as HIPAA Covered Entities, how they qualify is a little more problematic. HIPAA’s Administrative Simplification Regulations defines HIPAA Covered Entities as *“a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter”*.

Most, but not all, pharmacies transmit health information electronically. Pharmacies are generally considered health care providers.

The HIPAA Journal states that the complexity of whether a pharmacy is “covered” arises as follows:

Health care providers are defined in 45 CFR §160.103 as:

1. *“A provider of services (as defined in 42 U.S.C. 1395x(u)),*

2. *A provider of medical or health services (as defined in 42 U.S.C. 1395x(s)), and*
3. *Any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.”*

Most pharmacies do not qualify based on the first two criteria – 42 U.S.C. 1395(x) – either u or s. Most pharmacies do qualify based on the third category because health care is defined in the Administrative Simplification Regulations as including “[the] sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.”

This means that any pharmacy that does qualify as a covered entity must comply with HIPAA’s Administrative Requirements which include the Privacy Rule, the Security Rule, and “*if a breach of unsecured Protected Health Information occurs – the HIPAA Breach Notification Rule.*”

Pharmacies should already be familiar with these rules but periodic reviews can help eliminate mistakes and poor practices.

- **The HIPAA Privacy Rule.** This rule can be the hardest HIPAA rule to comply with for pharmacies because the rule may be hard for customers to ask questions and for pharmacists to answer questions – in retail environments – without being overheard and without disclosing PHI to the public.

“It may also be difficult to comply discretely with requests for a permitted disclosure from (for example) law enforcement officers.”

This means that employees of pharmacies need to be educated on what uses and disclosures of PHI are permissible and what standards must be met to protect the patient’s HIPAA rights. Pharmacy owners and managers also need to have policies in place to make sure each customer receives and acknowledges the receipt of the Notice of Privacy Practices. Each employee must also understand the contents of this Notice to “avoid unintentional violations of HIPAA.”

- **The HIPAA Security Rule.** This rule requires that covered entities implement safety measures to protect the “confidentiality, integrity, and availability” of electronic PHI. Pharmacy owners and managers (or a company compliance owner) must identify threats to the security and data that are likely to occur and “*protect that data and the computer systems used to store that data – from unauthorized access, alteration, theft, or other impermissible uses and disclosures.*”

All pharmacy members should take security training – even if they do not access PHI. The members of the pharmacy staff should also be subject to the pharmacy’s HIPAA sanctions policy.

- **The Breach Notification Rule.** This HIPAA rule mandates which procedures pharmacies must use to protect unsecured PHI if the PHI is exposed to a third party – such as being overheard in a retail setting. Generally, pharmacies need to notify the individuals whose PHI was involved and the HHS Office for Civil Rights. The notification should identify the breach including what occurred, what information was not protected, and what steps the pharmacy is taking to mitigate any harm. The individual should be given advice about what steps they can take to mitigate any harm.

Any use or disclosure (electronic, paper, or verbal) of PHI that is not authorized and not permitted is presumed to be a breach – unless the pharmacy can show that there is little likelihood that the Protected Health Information has been compromised.

Best Pharmacy Practices for HIPAA Compliance

While there is not one overall standard, each state has its own laws, and different pharmacies may operate differently. The HIPAA Journal recommends the following best practices for HIPAA compliance. We also recommend that you speak with our experienced healthcare compliance lawyers who will explain HIPAA’s provisions and the recommended ways for becoming compliant.

The best practices include:

- **The appointment of privacy and security officers.** Pharmacies can choose any staff member to be a designated privacy

and/or security officer. The responsibilities of this position include risk assessment, identification of confidentiality threats, and maintaining the integrity and availability of patient health information. The officer(s) should develop and implement HIPAA policies and procedures to reduce the risks to an appropriate level.

- **Ensuring that PHI is not disclosed impermissibly.** It's not just the deliberate disclosure of PHI in violation of HIPAA's Privacy Rule that is problematic. Pharmacies need to work to protect PHI information that is accidentally disclosed. Pharmacies need to create and implement policies and procedures to reduce the risk of all types of disclosures. *"Care must also be taken not to disclose more than the 'minimum necessary' PHI."*
- **Obtain authorizations when necessary.** Pharmacies need to disclose PHI if requested by a patient or the HHS' Office for Civil Rights. Pharmacies may use PHI for *"treatment purposes, requesting or receiving payment, and pharmacy operations."* All other disclosures and uses must be authorized by the patient – in writing – and before the PHI is disclosed or used.
- **Obtain business associate agreements.** If a third party needs to access PHI to perform a service on the pharmacy's behalf, that party is considered a *"business associate."* *"A business associate must provide reasonable assurances to the pharmacy, by means of a business associate agreement, that the requirements of HIPAA have been understood and that HIPAA Rules will be followed."*
- **Inform patients of the pharmacy's privacy practices.** Pharmacies should place their privacy practices in writing and share those written policies with their patients. Patients should sign that they have received these policies. The policies should inform the patient how they can complain if they think their HIPAA privacy rights have been violated.
- **Give patients copies of their PHI.** Patients have the right to see their PHI (subject to some possible exceptions) on requests made to the pharmacy.
- **Handle the disposal of PHI properly.** Prescription labels and other documents should be disposed of so the PHI cannot be reconstructed or viewed. *"Paperwork such as labels should be shredded, pulverized, pulped, or incinerated. ePHI on electronic devices must be permanently erased before disposal."*
- **Educate the pharmacy staff.** The staff and anyone who assists the pharmacy should be trained about HIPAA's Privacy and Security Rules if they may come into contact with any patient health information. These workers and volunteers should also be trained about any federal or state PHI rules that may be stricter.

Pharmacies generally qualify as "covered entities" under HIPAA and must therefore comply with HIPAA's Privacy Rule regarding patient health information (PHI), Security Rule regarding electronic PHI, and the Breach Notification Rule in case protected information is improperly used or disclosed. Best practices include appointing HIPAA compliance officers, making sure patients have written copies of their rights, obtaining authorizations when necessary, and entering into business association agreements with outside companies.

Pharmacies should contact Cohen Healthcare Law Group, PC to discuss their HIPAA compliance requirements. Our experienced healthcare attorneys advise pharmacies and healthcare practices about healthcare compliance laws and regulations.

Contact our healthcare law and FDA attorneys for legal advice relevant to your healthcare venture.