

HIPAA Compliance for Pharmacies – Violations and FAQs

March 8, 2024

By Michael H. Cohen

This is our second article about what pharmacies should know about complying with HIPAA. In the first part, we discussed which HIPAA rules apply to pharmacies, as well as the best practices for pharmacies to demonstrate HIPAA compliance. This article provides examples of HIPAA violations and the potential consequences of violations. This article also answers FAQs about pharmacies and HIPAA compliance.

GOT HIPAA? GET HIPAA? JOYCE EXPLAINS WHY AND HOW

Interview with an expert in healthcare privacy and security, both on the federal side with HIPAA, and the state side, especially California law.

What conduct by a pharmacy is considered a violation of HIPAA?

A few examples of HIPAA privacy violations include disposing of Patient Health Information (PHI) in the trash instead of shredding it, leaving prescription information in areas that can be accessed by the public, and disclosing any prescription information to third parties without patient's consent.

HIPAA violations include the following:

- **Unauthorized access.** This includes intentionally or accidentally accessing patient health information – without patient authorization or a legitimate need – thus violating the patient's privacy rights.
- **Improper disposal.** Pharmacies may be cited for HIPAA violations if they improperly or incompletely dispose of patient records, medication information, or prescription labels that potentially expose sensitive data to people who are not authorized to see the information.
- **Inadequate Physical Security.** This type of violation includes the failure of the pharmacy to develop and implement physical safeguards to protect Patient Health Information.
- **Improper handling of prescriptions.** Pharmacies may violate HIPAA if they disclose patient's prescription information to a third party without the patient's consent or failing to follow specific verification procedures, thus compromising the patient's confidentiality.
- **Failing to train the staff and volunteers.** Pharmacies need to educate and train their workers and volunteers about HIPAA's privacy, security, and breach notification rules.

What are the consequences for pharmacies that violate HIPAA's requirements?

According to the [HIPAA Journal](#), when the Health and Human Services (HHS) Office for Civil Rights (OCR) receives a complaint or a notice of a breach, the office will conduct a review to determine if an enforcement action is required. If OCR believes a violation has been committed, the agency has the right to impose a civil penalty.

Often, the Health and Human Services Office for Civil Rights will provide technical help to prevent future violations from occurring or require that the pharmacy implement a corrective action plan if the violation is attributable to an underlying culture of non-compliance.

In a small minority of cases the Health and Human Services Office for Civil Rights will impose a civil penalty. Depending on the severity (tier) of the penalty and the level of culpability, the HIPAA Journal states that the following penalties can be imposed (subject to any HHS changes):

- Tier 1 – Reasonable Efforts. The penalties range from \$127 – \$63,973. The maximum yearly penalty for each violation is \$1,919,173.
- Tier 2 – Lack of Oversight. The penalties range from \$1,280 – \$63,973. The maximum yearly penalty for each violation is \$1,919,173.
- Tier 3 – Neglect – Rectified within 30 days. The penalties range from \$12,794 – \$63,973. The maximum yearly penalty for each violation is \$1,919,173.
- Tier 4 – Neglect – Not Rectified within 30 days. The penalties range from \$63,973 – \$1,919,173. The maximum yearly penalty for each violation is \$1,919,173.

The Attorney Generals for the different states also have the authority to impose civil penalties for each violation. If a pharmacy's violations involves criminal activity, the violation may be referred to the US Department of Justice.

A few examples of violations and penalties, according to the HIPAA Journal, include the following:

- In 2009, CVS Pharmacy settled potential HIPAA violations with OCR for \$2.25 million after it was discovered that prescription bottles and receipts had been disposed of improperly.
- In 2010, Rite Aid Corp settled with OCR for \$1 million to resolve violations of HIPAA relating to the improper disposal of PHI.
- In 2014, Walgreens was fined \$1.4 million for the impermissible disclosure of a patient's PHI. A pharmacist shared a patient's PHI with her husband and at least three other people.
- In 2015, Cornell Pharmacy, a small pharmacy in Denver, was fined \$125,000 for the improper disposal of PHI.

Even if there is no civil fine, the costs of technical help and corrective action plans can be expensive. To minimize the risk of HIPAA violations and to help address all other compliance issues, pharmacies should speak with [experienced healthcare lawyers](#).

HIPAA COMPLIANCE IS NOT THE END OF LIABILITY FOR COMPROMISING PATIENT PRIVACY

You think you've got HIPAA compliance handled, in order to try to stay ahead of steep federal penalties, and then learn that is just the beginning of the story. HIPAA compliance itself is thorny. [...]

FAQs about Pharmacies and HIPAA Compliance

When could a pharmacy not be considered a HIPAA-covered entity?

While pharmacies generally are considered "Covered Entities" and must thus comply with HIPAA's Privacy and Security Rules

– some exceptions do apply:

- **A pharmacy doesn't transmit health information.** This may occur for example for campus pharmacies where a student's medical records may be considered part of the student's educational records under FEPPRA – the Family Educational Rights and Privacy Act.
- **A pharmacy doesn't send or receive health information electronically.** Paper and phone conversations that are not digital are not considered electronic communications under HIPAA.
- **A pharmacy exclusively sells or dispenses drugs, devices, or equipment for which no prescription is required.** If just one transaction involves a prescription, then *"every operation becomes covered by HIPAA."*

How does individually identifiable health information differ from Protected Health Information?

Individually identifiable health information is health information that alone or with other common identifiers could be used to identify an individual. When common identifiers such as an individual's name, date of birth, or address are stored in a designated record set with health information, the common identifiers and the health information become Protected Health Information.

When can a pharmacy be able to disclose PHI to law enforcement officers?

PHI generally includes a patient's name. The PHI could include their physical description. Pharmacies (and staff members) may be permitted (but generally are not required) to disclose PHI to law enforcement officers in the following six instances:

1. There is a court order, court-ordered warrant, or subpoena that requires disclosure.
2. To help identify a suspect, a missing person, a witness, or a fugitive.
3. An official request by a law enforcement official about a victim or someone suspected of being a victim of a crime.
4. To inform law enforcement that someone has died – if the pharmacist thinks that the death is due to criminal conduct.
5. When the manager of a pharmacy believes that protected health information is evidence of a crime that occurred on the premises.
6. When essential to inform law enforcement about the commission and nature of a crime not occurring on the premises, the location of the crime or crime victims, and the perpetrator of the crime.

Permitted disclosures of PHI to federal and state law enforcement officers are subject to the Minimum Information Necessary Standard.

What is the Minimum Information Necessary Standard?

The Minimum Information Necessary Standard requires that pharmacies (and pharmacy staff) should only use, disclose, or request the minimum amount of PHI necessary to achieve the objective of the use, disclosure, or request. A pharmacist, for example, doesn't normally need to send a patient's entire medical history to an insurance company to check if the patient is eligible for any prescriptions.

Which laws may be even more strict than HIPAA?

Most states have their own privacy and licensing laws that were enacted to protect patients. Many of these laws require even more stringent protections than HIPAA. For example, some laws also protect a patient's genetic or biometric data. Generally, the HIPAA requirements must be followed but state laws may need to be followed – if stricter protections are required.

Pharmacies should review with experienced healthcare lawyers any other federal compliance laws regarding patient privacy and any state compliance laws. For example, pharmacies may need to consider *"the confidentiality of substance abuse disorder patient records (42 CFR Part 2) and privacy requirements within the Combat Methamphetamine Epidemic Act, Food*

and Drug Administration Amendments Act, and Patient Protection and Affordable Care Act.”

Why should all people who work for a pharmacy undergo HIPAA security and privacy training?

In today's world, even employees who do not regularly access patient health information may be affected indirectly by a phishing email or malware which could provide an outsider with the credentials needed to access the pharmacy's computer system – including any PHI in that system.

HIPAA violations include unauthorized access to patient health information, the improper disposal of PHI, a lack of security, improper handling of prescriptions, and failing to train staff about HIPAA compliance. Fines may be imposed by the US Department of Health and Human Services and the local states for violating patient's healthcare privacy rights. A few commonly asked questions include when might a pharmacy not be considered a covered entity, when can a pharmacy disclose PHI to law enforcement, and what is the minimum information necessary standard?

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

Book a Legal Strategy Session Today

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