HIPAA Violations Checklist

Sponsored by The Compliancy Group

Due to the complicated language of the Health Insurance Portability and Accountability Act (HIPAA), the number of scenarios the Act tries to cover, and the sometimes-conflicting guidance provided by the U.S. Department of Health & Human Services, it is not surprising when misconceptions exist about what constitutes a HIPAA violation.

For example, while most HIPAA Covered Entities are aware it is not necessary for a data breach to occur in order for there to be a violation of the HIPAA Rules, some might not be familiar with the circumstances in which unauthorized disclosures of PHI are not considered to be HIPAA violations. The objective of this HIPAA violations checklist is to help explain why.

What is a HIPAA Violation?

A HIPAA violation occurs when there is a violation of the Privacy, Security, or Breach Notification Rules by a HIPAA Covered Entity or a Business Associate. Some breaches of the Health Information Technology for Economic and Clinical Health (HITECH) Act are also considered to be HIPAA violations when they relate to patient access requests.

As mentioned above, there does not have to be a data breach for a HIPAA violation to occur. If, for example, a Covered Entity fails to implement audit logs on computer systems that provide access to electronic Protected Health Information (ePHI), the Covered Entity is in violation of the Technical Safeguards of the HIPAA Security Rule - even if there is no unauthorized access of ePHI.

Because there are hundreds of ways in which it is possible to violate HIPAA Rules, it is not possible to list each one in our HIPAA violations checklist. However, in order to demonstrate the comprehensive range of potential HIPAA violations, our checklist includes many different types of example HIPAA violations that Covered Entities and Business Associates need to be aware of.

Example HIPAA Violations

Example HIPAA Privacy Rule Violations

❑ The failure to conduct HIPAA training for new employees, periodic training for existing employees, and additional training when there is a “material change in polies or procedures”.

❑ The failure to manage written paper charts or records and keep them out of public view in order to prevent the exposure of PHI to unauthorized third parties.

❑ The failure of obtain written authorization for the use or disclosure of PHI for reasons other than treatment, payment, healthcare operations, or those permitted by the Privacy Rule.

❑ The failure to prevent employees accessing patient files without authorization for motives of curiosity, spite, or to monetize data.

Example HIPAA Security Rule Violations

❑ The failure to enter into a HIPAA-compliant Business Associate Agreement with a Cloud Service Provider prior to saving ePHI in cloud object storage volumes.

❑ The failure to implement a mechanism that authenticates ePHI in order to determine whether data has been altered or destroyed in an unauthorized manner.

❑ The failure to encrypt ePHI, implement an alternative data protection solution that is equally as effective, or document why encryption is not considered necessary.

❑ The failure to implement electronic procedures that automatically terminates access to ePHI from computers and mobile devices after a period of inactivity.

Example HIPAA Breach Notification Rule Violations

❑ The failure to notify affected individuals within 60 days following the discovery of a breach of unsecured PHI/ePHI.

❑ The failure to provide a toll-free phone number that remains active for at least 90 days where individuals can learn if their PHI was exposed in the breach.

❑ The failure to alert the media to a breach of unsecured PHI affecting more than five hundred residents of a state or jurisdiction within 60 days of the breach being discovered.

❑ The failure to alert the Department of Health & Human Services to a breach affecting more than five hundred records within 60 days of the breach being discovered.

Unauthorized Disclosures Not Considered to be HIPAA Violations

Unauthorized disclosures of PHI not considered to be HIPAA violations should not be confused with examples of unintentional HIPAA violations. A HIPAA violation is a violation regardless of whether it was unintentional or malicious. However, both types of event can be avoided with effective training and due diligence. For example:

A technician accidentally opens the wrong patient file while carrying out their authorized duties. The unauthorized disclosure of PHI was both unintentional and in the course of the technician´s duties, so no breach has occurred - unless the technician later shares the content of the file opened in error with unauthorized third parties.

A clinic mails an Explanation of Benefits brochure to the wrong patient. The recipient - realizing the brochure is not for them - reseals it in the envelope and returns it to the clinic. Provided the clinic can be reasonably sure the recipient did not retain the information meant for another person, the unauthorized disclosure is not considered to be a HIPAA violation.

HIPAA Violation Fines

Fines for HIPAA violations are calculated according to the nature of the violation, how long it was allowed to continue after being discovered, the nature of any data accessed without authorization, and -

if data has been accessed without authorization - the number of people affected. Previous HIPAA violations can also be taken into account in the case of persistent offenders.

Fines can be layered on top of another if, for example, a data breach occurred (violation #1) due to the failure to automatically terminate access to ePHI (violation #2), the device from which data was extracted was left unattended due to a lack of training (violation #3), and the data was unencrypted at rest (violation #4). Thereafter, fines are issued according to the level of culpability:

Tier 1: A violation the Covered Entity was unaware of and could not have realistically avoided had a reasonable amount of care been taken to comply with the HIPAA Rules.

- Minimum fine per HIPAA violation (all amounts are for year 2019) - $117.
- Maximum fine per HIPAA violation - $58,490.

Tier 2: A violation the Covered Entity should have been aware of, but could not have avoided even with a reasonable amount of care.

- Minimum fine per HIPAA violation - $1,170.
- Maximum fine per HIPAA violation - $58,490.

Tier 3: A violation suffered as a direct result of willful neglect of HIPAA Rules in cases where an attempt has been made to correct the violation.

- Minimum fine per HIPAA violation - $11,698.
- Maximum fine per HIPAA violation - $58,490.

Tier 4: A violation of HIPAA Rules constituting willful neglect in cases where no attempt has been made to correct the violation.

- Minimum fine per HIPAA violation - $58,490.
- Maximum fine per HIPAA violation - $1,754,698.

DISCLAIMER

This HIPAA violation checklist is provided for information purposes only and does not qualify as legal advice. Understanding the causes of HIPAA violations can help Covered Entities and Business Associate better comply with the HIPAA Rules and avoid data breaches. However, understanding the causes of HIPAA violations does not guarantee that you or your organization are HIPAA compliant, and you should always consult a HIPAA compliance expert.