

Common HIPAA Mistakes and Steps to Prevent Them

[Richard P. Kusserow](#) | September 2024

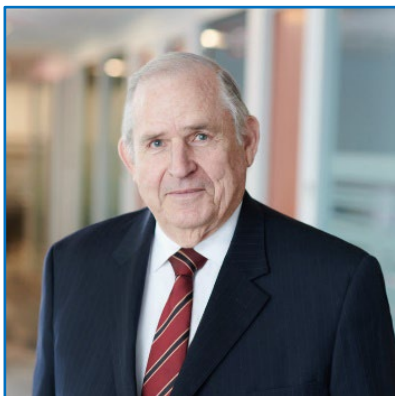
As of May 21, 2024, the Department of Health and Human Services, Office for Civil Rights (OCR) has received over 358,975 Health Insurance Portability and Accountability Act (HIPAA) complaints since the Privacy Rule's compliance date in April 2003. They have resolved 99% of these cases, or 356,075, and have started over 1,188 compliance reviews. HIPAA violations can be costly, with penalties that can include huge fines and even jail time. Most breaches are related to HIPAA violations including, (1) failure to secure and encrypt data, (2) device theft, (3) employee misconduct, (4) improper record disposal, (5) non-compliant partnership agreements, (6) failure to perform an organization-wide risk analysis, and (7) inadequate staff training. HIPAA violations can be discovered in several ways during data breach investigations. When a data breach occurs, OCR or a state attorney general may investigate the incident to determine if any privacy violations occurred. Common mistakes involving Protected Health Information (PHI) occur for a variety of reasons, including:

- **Inadequate Employee Training.** Given that staff training prevents nearly every other item on this list, it will come as no surprise that inadequate training is one of the most common HIPAA violations each year. There is simply no substitute for getting your staff properly HIPAA-trained and verifying that they fully understand the rules and how they apply.
- **Improper Disposal of Patient Information.** The failure to properly dispose of paper records or electronic devices containing sensitive information is a common problem. Items such as hard drives and USB drives that have not had PHI wiped or destroyed.
- **Unauthorized Access/Disclosure.** This continues to be a major cause of HIPAA breaches that may come about as a result of accidental third-party disclosure and human error.
- **Employee Snooping.** Employees often go through PHI for personal reasons. The government does not take snooping lightly and is aggressively taking action against wrongdoers, including in some cases in criminal prosecutions.
- **Absence of Patient Consent.** Lack of patient consent can be a potential HIPAA violation, but it is important to note that HIPAA regulations generally allow it for treatment, payment, and business operational reasons.

Tips on how to prevent violating HIPAA

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI and identify areas that need improvement.
- Develop a risk management plan to identify and address the identified risks.
- Implement policies and internal controls on document and device handling and PHI security.
- Store PHI data storage under lock and key during and at the end of its use.
- Ensure PHI is wiped from USB and drives when they are no longer needed.
- Provide continuous training regarding how to handle PHI and what constitutes a violation.
- Implement safeguards to prevent unauthorized access to PHI (e.g., access and audit controls, and encryption).
- Regularly review and update risk analyses for new risks or vulnerabilities warranting action.
- HIPAA violations can result in severe consequences for both patients and healthcare organizations. It is essential to understand HIPAA requirements and take appropriate measures to protect PHI and avoid violations.

You can keep up-to-date with Strategic Management Services by following us on [LinkedIn](#).



About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.