HIPAA Violations Continue to Increase

Richard P. Kusserow | September 2023

During the COVID Pandemic there have been many unintended violations involving PHI

HIPAA has been on the books for nearly 30 years, but violations involving protected health information continue to increase. This is because even organizations that implemented HIPAA Privacy and Security programs continue to risk violations. Since OCR took on the responsibility for enforcing HIPAA compliance, they have received over 300,000 rule violation reports. Over $134 million in fines have been imposed to date. In addition to their enforcement actions, OCR has referred over 1,700 matters to the DOJ for possible criminal investigation. During the COVID-19 Pandemic, many misunderstood the handling of Protected Health Information (PHI), which resulted in unintended violations. Common areas where violations occur include the following:

1. The most commonly reported violations are impermissible use and disclosures, access, administrative safeguards, and breach notifications. It is often the result of an organization accidentally accessing or releasing PHI. This frequently occurs when staff discuss a patient in an area so that unauthorized persons overhear it. The most effective means to reduce this problem is through training.
2. Other common violations involve failure to properly manage information with required authorization codes or identity verification. Implementing employee email can provide minimum employee verification. Cybersecurity training and best practices also go a long way to mitigate this risk. It is important to stress verifying the requested information before transmitting it. Even when the correct patient record is provided, if the individual has authorized only parts of their medical record to be disclosed, but the entire record was shared, that's a violation.
3. Another common way for PHI to be accessed by unauthorized individuals is through misplaced or stolen devices like laptops, USB drives, tablets, and smartphones. Since most

of this exposure is limited to the number of patients on these devices, the publicity and reporting are not as publicly visible. Devices from healthcare organizations typically contain sensitive patient information, and healthcare professionals often take work devices home and leave them unattended in their homes, cars, or public areas. This creates a situation where these individuals can lose, and unauthorized individuals can easily steal or access these devices. Prevent PHI disclosure when a device is lost or stolen by: (a) ensuring device encryption, (b) ensuring electronic PHI (ePHI) encryption, (c) installing device tracking software, (d) training employees regarding the handling of devices, (e) requiring password protection, and (f) active monitoring of systems and devices.

4. Improper disposal of sensitive patient information is another common violation area. This may involve failing to dispose of PHI and ePHI properly, including throwing away complete copies of PHI without shredding or failing to wipe ePHI from USBs or portable hard drives. To avoid this problem, there should be routine shredding of hard paper copies of PHI and destruction or data wiping of portable devices that store PHI.
5. Third-party risk is another problem area, as nearly all healthcare organizations work with third-party companies, many of which require access to PHI. Any company that has access to or handles PHI is required to be HIPAA-compliant. Third-party vendors that do business with healthcare organizations need a business associate agreement (BAA) before they access PHI. A BAA helps protect PHI by legally binding HIPAA-covered organizations and third-party vendors, which may not already be set up to handle sensitive healthcare information.

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.