STRATEGIC MANAGEMENT SERVICES

Tips To Avoid Common HIPAA Violations

Richard P. Kusserow | July 2024

Eight out of ten healthcare organizations have HIPAA privacy as part of their compliance program for guarding patient protected health information (PHI), and this is proving to be a significant added challenge. Violation of HIPAA privacy is the number one cause of encounters with regulatory and enforcement agencies. Penalties for failing to comply can be as much as $1.5 million.

Developing a strong compliance program should include plans to address the most common weaknesses that give rise to violations, such as:

Improper access to PHI. Employees gaining unauthorized access to patient information is a common problem that exposes the organization and the individual to enforcement action and penalties. Addressing this problem requires written policy guidance and training to ensure everyone understands the rules and the consequences of not following them.

Lost/Stolen Mobile Devices. Mobile devices (tablets, smartphones, and flash drives) are common tools used by providers in the healthcare sector. They permit clinical staff to gain access to critical information that enables timely decisions in providing care to patients. However, data security is a problem for mobile devices, particularly as they have a greater risk of loss or theft. Lost and stolen devices are the number one reason for patient data breaches of more than 500 records, and unauthorized access to PHI on a device would be considered a HIPAA privacy violation. Some steps to avoid a problem with lost or stolen devices are to: (a) develop policy guidance and training regarding mobile devices and PHI; (b) require a passcode to access information on the mobile device; (c) require logging in each time information is accessed; and (d) download an encryption app to the devices to protect information.

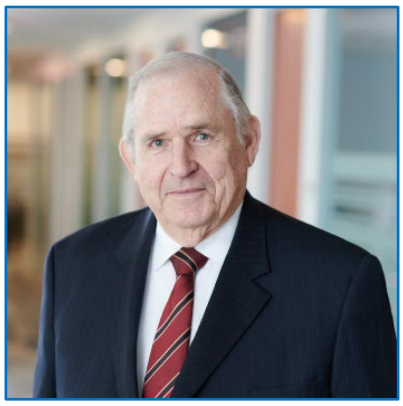
Disclosing of Information. The number one cause of HIPAA violations are employees who disclose personal information about a patient. In some cases, it is a willful act, but mostly it results

from carelessness or ignorance. Acts by employees create liability exposure for both the organization and the individual. It is important that those employees who have access to PHI are properly trained and retrained on how to avoid improperly disclosing PHI.

Mishandling of patient records. It is essential for healthcare providers to properly handle medical records. There must be specific compliant security measures, policies, protocols, and clear access control priorities. Even with solid written guidance, there is a dependency on employees following it.

Training Failure. All of the above issue areas tie into the importance of proper training on HIPAA compliance. Not only must employees know what is expected of them in complying with guidance, but failure to follow the rules may result in adverse actions being taken. The HIPAA Privacy Rule states that training must be provided to "each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce." The purpose of HIPAA training is to ensure all members of the workforce that interact with (PHI) are aware of the policies and procedures covering that information, including the permissible uses and disclosures, how to safeguard that information, patient rights, how to work in a HIPAA-compliant way, and what happens if HIPAA is violated. Periodic retraining is also a must to ensure important messages are not forgotten.

You can also 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.