CampusGuard News 3/1/2020

HIPAA: Common Violations and How to Avoid Them

Not only does a breach of healthcare information land you on HHS's Wall of Shame (OCR Breach Portal), failure to comply with HIPAA can lead to significant financial penalties. Continued education with all staff that are accessing, storing, or transmitting protected health information (PHI) is key to avoiding this undesirable distinction. Although many data breaches are caused by cybercriminals or other risks like malware, ransomware, and phishing, breaches are also due to employee behavior and a failure to follow defined procedures.

A few of the more common (and preventable!) incidents that can lead to breaches of protected health care information include the following:

- **Insider Snooping**
  Employees snooping on healthcare records of family, friends, and celebrities is, unfortunately, a very common HIPAA violation. Accessing the health records of patients for any reason other than treatment, payment, or healthcare operations, as permitted by the Privacy Rule, is a violation of patient privacy.

  Staff should not be accessing patient records that they are not authorized to view or that they do not have a legitimate need to open. Employees should not even access their own medical records using their employee login credentials. They should obtain copies of their individual health records following the same request procedure as every other patient.

  Most organizations now have EHR systems in place to monitor and log user activity, and are tracking which medical records are accessed, what was viewed, how long the record was open, etc. This allows organizations to easily identify misuse and take appropriate actions. If caught snooping, employees are usually terminated, but they can also face criminal charges. An organization that fails to prevent snooping can also face financial penalties.

- **Inadvertent Sharing**
  Employees must take precautions to ensure they do not accidentally share sensitive patient information. Employees should protect patient information just like they would want their own sensitive information protected and follow these simple best practices to ensure it does not end up in the wrong hands (or ears).

    - Do not share or discuss PHI with others who shouldn't have access to it, including co-workers.

- Avoid accessing patient records unless needed for work.
- Minimize the chances of others overhearing patient information. Do not use a patient's whole name within hearing distance of others.
- Never leave PHI unattended. Secure all paper documents containing PHI by placing in a locked drawer or cabinet when not in use. Cover charts so patient names are not visible.
- Close and log out of computer applications containing patient information.
- Never e-mail PHI data.

- **Removing PHI from a Healthcare Facility**
  Another common employee HIPAA violation is to email PHI to personal email accounts in order to access that information remotely. Even with the best intentions (e.g., completing work tasks after hours), using personal computers or laptops to access patient records places that information at risk of accidental exposure. Downloading PHI onto unauthorized devices can also present compliance concerns as these devices may not be secure, and can create potential privacy and security risks. There is always the risk of personal devices being lost or stolen. To avoid these potential violations, create clearly defined policies for accessing PHI on personal or mobile devices, and verify all employees have been educated on these guidelines.

- **Sending PHI to Wrong Contacts**
  Organizations will find themselves in trouble if patient information is accidentally sent to the wrong person, either through mail, e-mail, or via fax.

  Last year, Sentara Hospitals agreed to take corrective actions and pay a $2.175 million to settle HIPAA violations. The incident came to light when HHS received a complaint alleging that Sentara had sent a bill to an individual containing another patient's PHI. OCR's investigation determined that Sentara had mailed 577 patients' information to the wrong addresses. Sentara only reported this incident as a breach that affected 8 individuals because they incorrectly concluded that unless the disclosure included patient diagnosis or treatment information, no reportable breach had occurred. Even after being advised of their duty to report the others affected, they refused. This is an example of how a simple mistake became a violation costing millions of dollars.

  Employees should always double check the address or phone number before reaching out to a patient with sensitive information, and verify the patient information before sharing details over the phone if the patient has called in.

- **Failure to Evaluate Business Associates**
  The single largest breach in the first half of 2019 was a hacking incident affecting over 20 million patient records that involved the American Medical Collection Agency, a third-

party billing collections firm. It's estimated that the number of patients' data potentially exposed by the breach is now over 22 million.

26% of data breach incidents involve a business associate or third-party vendor. Business associates can be fined directly by regulators for HIPAA violations. However, if a covered entity fails to obtain satisfactory assurances that a Business Associate is HIPAA-compliant prior to entering into a contract, and a breach of PHI occurs, the covered entity may then be considered liable for the breach.

The failure to enter into a business associate agreement with all vendors that are provided with or given access to PHI is a common HIPAA violation. In recent years the OCR has been more aggressive in enforcing these penalties. Phase two of OCR's HIPAA audit program that launched in 2016 also started included selected business associates.

Organizations should carefully vet all vendors, and outline security and privacy expectations in detail. With 45% of business associate breaches caused by outside hacking, verifying that the appropriate security controls are in place with everyone you share PHI with is critical. All third-parties should undergo a thorough review before procurement, and agreements should be updated as requirements or processes change. When you think about it, your organization's privacy and security is technically only as good as your weakest business associate. (…or employee!)

- **Failure to Perform an Organization-Wide Risk Analysis**
  The failure to perform an adequate organization-wide risk analysis is one of the most common HIPAA violations that is penalized/fined by the OCR. If a risk analysis is not performed regularly, organizations struggle to determine if vulnerabilities to the confidentiality, integrity, and availability of PHI exist. Performing a risk analysis should not just be a checkbox item for compliance; conducting a well-planned and well-executed analysis benefits the whole organization. Risks that are identified during the assessment should be prioritized and addressed in a reasonable time frame.

Being HIPAA compliant is not just about preventing data breaches. HIPAA compliance is about protecting the sensitive health information of your patients and reducing the risk of a breach to an appropriate and acceptable level. In fact, the HIPAA fine structure is based on the organization's level of culpability and perceived negligence associated with the HIPAA violation. Organizations that have taken measures to meet HIPAA's requirements will face a much smaller maximum penalty than those who are found negligent. It is critical for HIPAA-covered entities to stress the importance of protecting PHI with their staff, conduct regular HIPAA compliance reviews to make sure any violations are discovered, and to correct those violations before they are identified by regulators or taken advantage of by criminals.

Additional guidance from our Security Advisor and Customer Relationship Manager teams below:

[Coudeyras]: *Without proper education and training in place, many employees do not understand their responsibilities for HIPAA. Creating a strong culture of security awareness is key to protecting sensitive data. Technical controls can be bypassed by employees who make simple mistakes that can have dire consequences. Therefore, building security into "business as usual" processes is necessary.*

[Johnson]: *As the number of confirmed cases of COVID-19 continue to increase, it is important to educate staff on how and when PHI may be disclosed. The HIPAA Privacy Rule specifically authorizes covered entities to disclose requested PHI to public health authorities if a person is at risk of contracting or spreading a disease. Health care providers can share PHI in order to prevent or lessen a serious and imminent threat to the public health and safety. However, it is important that in these situations, providers are making a reasonable effort to only disclose the patient information necessary and protect against any intentional or unintentional uses in violation of HIPAA. Specific information about identifiable patients should not be shared with the media or the public at large. Remind employees they may only access PHI as they have been authorized to do so to carry out their jobs.*