HealthITSecurity
News and Resources for HealthIT Security Pros

# How Administrative Safeguards Can Prevent Data Breaches

Preventing healthcare data breaches is a common goal for covered entities of all sizes. It can be easy to let the importance of administrative safeguards fall behind other areas, such as concerns over hacking and stolen devices, but organizations need to keep this aspect a key part of their larger data security plan.

According to the Department of Health and Human Services, administrative safeguards are "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

***"...compliance...will require an evaluation of the security controls already in place, an accurate and thorough risk analysis, and a series of documented solutions derived from a number of factors unique to each covered entity."***

However, healthcare organizations need to adopt administrative safeguards that are applicable to their daily operations. For example, policies and procedures that dictate employee training at a small doctor's office will likely not be applicable to a large hospital.

"...compliance with the Administrative Safeguards standards will require an evaluation of the security controls already in place, an accurate and thorough risk analysis, and a series of documented solutions derived from a number of factors unique to each covered entity," explains the HHS Security Series.

*Both **covered entities and business associates** should know how administrative safeguards can assist in preventing healthcare data breaches. From there, they can implement the necessary measures to create a comprehensive and current approach to data security.*

## Employee training, regular education programs

Workforce security training will have a large impact on how an organization can keep ePHI secure. Employees at all levels need to understand the covered entity's "security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures," according to HHS.

Several healthcare data breaches from the past year were caused by human error. For example, several providers reportedly **mistakenly faxed health data** files to a New York marketing firm instead of to Quest Diagnostics.

A report by the law firm Baker Hostetler found that **human error was the number one cause** of data security issues. Specifically, employee negligence was responsible for 37 percent of reported issues.

Healthcare breaches were also found to be the most frequently reported incidents, according to the law firm, which was likely due to federal data breach notification requirements.

Beth Israel Deaconess Medical Center CIO John Halamka, MD, MS, **explained earlier this year** that healthcare organizations are "as vulnerable as our most gullible employee."

"We spend millions on new technology, countless hours on policy writing, and engage all stakeholders to enhance their awareness," Halamka wrote in a blog post. "Yet, we're as vulnerable as our most gullible employee."

Employee training cannot be overlooked. Individuals need to understand how to recognize malicious activity - such as **phishing scams** - and how to appropriately respond. Staff members should also receive regular security training, so that even as technology evolves and a facility adopts new devices, they still know how to protect ePHI.

## Understanding information access management

Employees should only be given access to ePHI as it relates to their job, and that is "the minimum necessary" to ensure that the job is performed correctly.

"Restricting access to only those persons and entities with a need for access is a basic tenet of security," states the HIPAA Security Series. "By implementing this standard, the risk of inappropriate disclosure, alteration, or destruction of EPHI is minimized."

Moreover, healthcare organizations need to "evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information."

For example, a doctor or physician will likely need greater access to patient records than an individual who works in medical billing. The latter employee might not necessarily need access to a patient's medical history, and instead just needs to see the patient's address and billing information.

This is also where healthcare organizations need to consider access privileges to workstations, transactions, programs or processes. Should an employee choose to leave his or her position, or the employee is fired, then access should also be terminated. Otherwise, an organization runs the risk of unauthorized access.

Marty Edwards, MS, CHC, CHPC, Compliance Officer at Dell Services Healthcare and Life Science division, **told *HealthITSecurity.com* earlier this year** that "the human factor" is critical for any healthcare organization.

"You have to keep in mind that all the users who have access to that data have a role or responsibility, and are using that information for a specific purpose," Edwards said. "So it's up to those users to make sure they follow the necessary processes, procedures and policies in place for the disclosure of that information."

## Working with business associates

Business associates who create, receive, maintain or transmit ePHI should have a written contract or arrangement that meets the applicable requirements of HIPAA. Otherwise, there can be confusion following a healthcare data breach.

Medical billing services, hardware and software vendors, external consultants, and lawyers could all be considered business associates.

Healthcare organizations need to know whether or not there are existing business associate contracts, and if ePHI is involved. From there, it can be determined if Security Rule requirements need to be addressed.

Business associates can also experience a data breach, and without the proper documentation, it will be more difficult to prove which facility is responsible.

For example, Triple-S Management Corporation **agreed to an OCR HIPAA settlement** earlier this year that included a $3.5 million fine. One of the areas in which Triple-S was found to be non-compliant had to do with an outside vendor.

OCR found there was "impermissible disclosure of its beneficiaries' PHI to an outside vendor with which it did not have an appropriate business associate agreement."

## Regular evaluations to maintain compliance

Overall, covered entities should have ongoing monitoring and evaluation plans. Administrative safeguards, along with the rest of the data security plan, should be periodically reviewed. That way, organizations can adjust to any environmental or operational changes that affect ePHI security.

Current policy and procedures should be implemented to ensure proper management and execution of security measures. As highlighted by the HIPAA Security Series, this includes "security management process, assignment or delegation of security responsibility, training requirements, and evaluation and documentation of all decisions."

Administrative safeguards will not guarantee that a data breach will never take place, but they will keep an organization compliant and are an important step to ensure ePHI security.

Article by **Elizabeth Snell** December 29, 2015 posted at: http://healthitsecurity.com/news/how-administrative-safeguards-can-prevent-data-breaches