Three Steps to Prevent Information Breaches at your Health Care Organization

healthcarebusinesstoday.com /three-steps-to-prevent-information-breaches-at-your-health-care-organization/

Healthcare Business Today Team

By Ken Carter

Protecting patient information is one of the most important things hospitals and health care systems can to do to maintain an excellent level of care. Implementing basic preventative security precautions goes a long way in maintaining a secure environment where both your patient and organizational information is safe. Now more than ever, it is critical to stay proactive about protecting your patient and organizational information.

Here are three basic yet vital steps every organization should be taking to prevent information breaches at health care facilities.

Perform a full, holistic risk assessment

Before you can be fully prepared meet today's security challenges, you need to understand where the potential vulnerabilities within your organization lie. Assessing your organization's risks and auditing the existing processes is a vital first step in determining any potential weaknesses.

Approach your organization's information protection from a holistic perspective, and ask yourself about every possible way a criminal might gain access to patient or business information. Though every health care organization has the same concerns about patient information, each individual facility will face different challenges based on their structure.

Ultimately, a comprehensive risk assessment helps organizations limit and prevent access to patient information. A proper risk assessment can not only establish and improve your existing policies, but also impact and improve staff behavior.

Properly screen and train your employees

The biggest threat that a health care organization can face is sometimes an internal one. Employees are at the core of the health care business, and they are also the ones with the most access to patient records and information. Because health care is person-driven and patient-centered, organizations are only as good as the people they employ.

For new employees, it is important to screen and verify every staff member before you hire them. Everyone from physicians to administrative and support staff need to be properly screened and undergo a comprehensive background check that includes verification of their licenses and credentials.

For your current and existing employees, continue annual training on HIPAA and privacy awareness. Your employees need to understand the legal implications for patient privacy and how they can better protect information during their day-to-day job responsibilities. A proactive approach to annual training and assessments will result in highly trained employees who will also be able to recognize organizational vulnerabilities.

Limit information access physically and electronically

Establish policies and controls to restrict access both physically and electronically to authorized personnel only. You want to prevent a person from accessing electronic information they have no legitimate reason to access.

Health care organizations have done a good job of responding to new technologies and the potential vulnerabilities they may create, but securing physical access to your organization is just as important. Implement badging and lock systems so only certified personnel have access to sensitive areas. Setting multiple levels of access will allow for further control of who has access to specific areas of your facility.

In addition to limiting physical access to information, limit electronic access to your organization's network and systems. Grant electronic access to authorized users only, and set up automatic password change requirements every 90 days or sooner. Set policies for personal devices like smart phones and tablets, and require safety precautions like anti-virus software for employees who need to use them on the job.

Your organization may also want to implement technologies such as fingerprint or iris scanners. These tools can be used as both physical and technology safeguards, to assure that only specific individuals have access to sensitive information.

Securing your organization and patients' information is never a one-step process. It is continuous, and needs to be updated regularly as your organization grows, hires new employees or implements new changes in technology. Criminals will search for the path of least resistance and the easiest means of access to company information, so it is important to protect yourself on all fronts. The more proactive your organization can be, the more secure it will be.

Ken Carter is the Vice President of Central USA at Pinkerton, with over 23 years of experience in investigations and security consulting with health care organizations around the country. Pinkerton is a global, holistic risk management agency that offers consultation, investigative and protective services, employment screening and protective intelligence. For more information, visit: www.pinkerton.com.