RISK INSIGHTS

GILBERT INSURANCE GROUP
"WE CONNECT YOU TO YOUR MOST VALUABLE INSURANCE SOLUTION"
480-926-9030 www.gilbertinsurancegroup.com

HEALTH CARE

Protecting Patient Data by Preventing Cyber Attack

The threat of a data breach in a health care facility is daunting. Privacy is the foundation of hospitals' information systems, and compliance with the Health Insurance Portability and Accountability Act (HIPAA) – along with the facility's reputation – will be jeopardized if just one patient's information falls into the wrong hands. Health care facilities are particular targets for two reasons:

- *Type of data stored*: Health care facilities may keep a patient's social security number, insurance and financial account data, birth date, name, billing address and phone, making them a valuable target for cyber attack.
- *Many potential vulnerabilities*: Health care facilities are obligated to provide access to several external networks and Web applications in order to stay connected with patients, employees, insurers or business partners. The volume of data shared represents a risk.

It is much less costly, both from a financial and reputational point of view, to prevent a cyber breach than to notify individuals and the Department of Health and Human Services of a breach as required by HITECH. As a result, administration must respond by preventing, detecting and responding to cyber attacks or misuse of patient records through a well-orchestrated cyber security program.

Health care facilities are particular targets for cyber attack because of the extent of data stored and the amount of access provided to external networks.

What are the Risks?
The first step in protecting your business is to recognize the parts of your processes that are prone to cyber attack.

Applications and Systems
External applications and systems are ripe for improper access to sensitive patient data. Since administrators do not have complete control over the security of external applications, facilities should perform Web application security testing on a regular basis.

Software Flaws
Weaknesses in software and computer systems attract hackers and intruders. The results of this cyber risk can range from minimal mischief (creating a virus with no negative impact) to malicious activity (stealing or altering information). Intrusion prevention and detection systems can alert you of cyber attacks and allow you to respond in real time.

Malicious Code (viruses, worms and Trojan horses)
- Viruses: This type of code requires that the user take an action before it can infect your system, such as open an e-mail attachment or go to a particular Web page.
- Worms: This code propagates systems without user intervention. They typically begin by exploiting a software flaw or weakness. Once the victim's computer is infected, the worm will attempt to find and infect other computers.

- Trojan horses: This code is software that claims to be one thing while it is acting differently behind the scenes (program that claims to speed up your computer system but is actually sending confidential information to a remote intruder).

Implementing systems of preventing these attacks, including firewalls and regular security controls is essential to protecting sensitive data.

E-mail Lacking Encryption
HIPAA guidelines require that some e-mail communications with physicians' offices and hospitals be encrypted to protect patient information. Since most communication is now electronic, monitoring these means is especially important.

Insider Attack
Current or former employees ranging from billing clerks to clinicians should understand that the consequences for consulting patient records without a valid cause can range from serious punishment to termination. Often employees are simply curious, and only a severe policy can effectively prevent this type of data loss. Many facilities implement log monitoring, for which logs of access to sensitive patient data are regularly reviewed.

Physical Loss of Information
Another potential risk is that of lost or stolen laptops, which lead to missing personal information related to patients or employees.

In the event of a security breach, the HITECH Act calls for notification of the individuals concerned and HHS in a short time span.

Risk Management
In the case of a surprise Health and Human Services (HHS) HIPAA inspection, facilities must prove that they are compliant with all regulations and requirements outlined in HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

To reduce your facility's cyber risks, it is wise to develop a comprehensive Risk Management Plan. Risk management solutions utilize industry standards and best practices to assess hazards from unauthorized access, use, disclosure, disruption, modification or destruction of your facility's information systems. Thereafter, perform regular security risk assessments, which will give you a better understanding of the risks posed to your protected health information and personally identifiable information identified in these two acts.

You should also examine the controls in place at your facility to ensure they are sufficient for regulatory requirements. Executing this process helps your organization remain in compliance and demonstrates diligence and a commitment to compliance in the case of an audit.

Consider the following when implementing risk management strategies:

- Create a formal, documented risk management plan that addresses the scope, roles, responsibilities, compliance criteria and methodology for performing cyber risk assessments. This plan should include a characterization of all systems used at the organization based on their function, the data stored and processed and importance to the facility.
- Perform security risk assessments at least on an annual basis and update it whenever there are significant changes to your information systems or the facilities where systems are stored, or when there are other changes that may impact the vulnerability of the organization.

Selecting an ISP
In addition, your organization should take precautionary measures when selecting an internet service provider (ISP), which provides access to the Internet, website hosting and other services. To select the ISP that will best reduce your cyber risks, consider the level of security, privacy and reliability it offers.

Transferring the Risk
Cyber security is a serious concern for all health care facilities. Contact Awesome Agency to learn about our risk management resources and insurance solutions, such as Internet/Media Liability, Security and Privacy Liability and Identity Theft Insurance today.