

## **Is the Security of Your IT Systems Up to HITECH Requirements?**

HITECH Act of 2009 addressed the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. As the adoption of information technology (IT) increases and more providers move towards using electronic health records and enterprise-wide information systems, data security and privacy will become more important than ever for long-term and post-acute care providers. Dennis Stuftt, president and CEO of Prelude Services, in partnership with LeadingAge CAST, compiled a list of questions and considerations for data security that should be in place within provider organizations. The list is a result of years of experiences Dennis spent managing IT.

### **IT Security Questions You Should Ask**

As our industry gets closer to electronic health records, and the risk associated with HIPAA disclosure issues increase, there are several questions you should ask your IT department and vendors. Answers to these questions will help you assess the gaps in your IT systems and the level of risk that they pose.

The responsibility of IT security policies and procedures go beyond the IT Department. IT security policies have implications for human resources, privacy and corporate compliance that you need to carefully review to determine what is the applicable security standard and the appropriate actions to address the existing gaps. These questions represent a number of best practices Prelude Services implemented for its clients.

Individual security access to data is controlled predominately with a user name and password. There are other means of access with control systems, access cards, key fobs and biometrics. Some access control questions to ask are:

- ◆ How is individual user access to the network and software granted, documented, and monitored?
- ◆ Is there a tracking system for reviewing access requests when new employees are hired, access permissions are changed, and when employees leave the organization?
- ◆ Are employees outside of IT responsible for granting user access to financial and clinical systems?
- ◆ Do passwords have to be changed periodically and must they contain a combination of letters, numbers and symbols?
- ◆ Are servers located in a secured room and is access restricted to employees that need access based on job functions?

Consider a manual or automated process for business units or human resources to submit a written request to IT to add, change or delete network accounts. IT should then keep a log of completed requests. Consider having designated staff outside of IT add, change, or delete user access within financial and clinical systems.

IT should also set-up a strong password format that enforces the format of passwords, and requires all passwords to be changed on a set interval of time. Restricting access to the server room is another consideration for protecting your data.

You should also have several key IT operational policies and procedures in place to protect your data. The data security management questions you should ask are:

- ◆ Is data backed-up every day?
- ◆ Are the back-up copies stored off-site in a secured facility?
- ◆ Do you monitor the back-up process and periodically test restoring data from a back-up copy?
- ◆ Is there a written and tested disaster recovery plan for IT?
- ◆ When you dispose of PCs, laptops, servers, network electronics, smart phones and copiers to a third party, do you delete your data and have a policy statement from the third party on their disposal policy?
- ◆ Do you have a data retention policy for how long e-mails are saved or archived?

An easy and costly mistake for IT to make is assume the daily backup processes are working because there are no errors generated. IT needs to verify these critical processes work every day to insure data is being copied from the server to another form of storage media. Copying mission-critical data to storage media that can be stored at an off-site facility is also highly recommended as a way to recover from a damaged or inaccessible server room. These backups can only be used to restore your business systems in a timely manner if IT has an alternate site with compatible servers for downloading your data. Ask IT how long it would take to prepare new servers to load your data on them, and to establish remote access from a different location. Having a disaster recovery plan that is tested periodically is the only way to make sure you can use the written plan to restore data and operations.

Have you ever heard IT make the statement “delete delete?” Data can be deleted from a device and still be physically stored on the device. You should consider using methods that are available to wipe a device clean before it leaves your facility. Copiers and most electronic devices store data in digital form that can be viewed unless you make certain it is really deleted. Make sure your vendors have a written policy for removing your data before devices go to a third party, and ask for a copy of their policy. Also consider asking for a certificate from a third party that guarantees PCs, servers, and printers will be disposed of within the proper environmental disposal regulations after they leave your facility.

Other areas within IT to question are network access, Internet access, PCs, laptops and handheld devices. Some key questions to ask are:

- ◆ Can anyone who is not an employee, including residents, plug into a network connection or access a wireless network and obtain access to the Internet? If they can, is this access separated from your internal business network?
- ◆ Do you allow employees to connect to their PC or laptop in the facility remotely over the Internet?
- ◆ Do you monitor employee Internet usage?

- ◆ Do you restrict what sites employee can get to on the Internet?
- ◆ Do you allow employees to forward their e-mail to a personal e-mail account?
- ◆ Do you have a way to delete e-mails on a smart phone that is lost or stolen?
- ◆ Do you have a way to send e-mail outside of your organization in a secured manner for e-mails that contain protected health information within the body of the message or in attachments?
- ◆ Do you restrict who can use a thumb drive or disk drive on a PC or laptop, as well as what may be downloaded?
- ◆ Do you have a policy for what data can be stored on a PC, laptop, or handheld device that is used outside of the facility?
- ◆ Do you encrypt data on laptops or tablets that store protected health information on their hard drive?
- ◆ Do you have a policy for employees to log off when they leave a workstation?
- ◆ Do you enforce a screen saver policy that will automatically lock an unattended computer after a set period of time?

Access to the Internet by employees and residents will only increase in the future. Hardware and software tools are available to restrict, monitor, and control what can be accessed and downloaded onto and off of your network. These tools are an integral part of your IT system and will help reduce your exposure to network attacks and the accidental loss or disclosure of sensitive data.

All of these system protections can only be effective if employees are trained and if such policies are enforced. Therefore, proper employee and supervisor training on HIPAA, privacy, data security, and use of all electronic devices are critical to a successful program.

Answers to these questions should help you determine what security and management procedures are right for your organization. These answers can help guide you to raise your level of data integrity and lower your risk exposure.

### **About the Author**

Dennis Stufft has more than 30 years of management, information technology, and consulting experience in the health care and financial industry. Since 1998, he has served as the president and CEO of Prelude Services, an IT services company who provides IT services for the senior and community services industry. He is also a LeadingAge CAST Commissioner.

Contact Dennis Stufft at [dstufft@preludeservices.com](mailto:dstufft@preludeservices.com) for additional information.