International Journal of Economics, Commerce and Management
United Kingdom Vol. V, Issue 10, October 2017
http://ijecm.co.uk/ ISSN 2348 0386

SECURITY OF INFORMATION AS A PART OF THE HOSPITAL WORK

Tsvetomir Dimitrov
First Multiprophy Hospital for Active Treatment, Sofia, Bulgaria
dimitrov.tzvetomir@abv.bg

Zahari Goranov
Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre
Bulgarian Academy of Sciences, Sofia, Bulgaria
zgoranov27@e-dnrs.org

Abstract

The purpose of this report is to show the importance of information as part of the work of the hospital. The ways of prevention, as well as the preservation of the information are considered, which in turn is a prerequisite for the development of the state. Good prevention practices applied around the world are shown. Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. The security of information is also very important for the patients. If someone obtains patient-sensitive information, they can use it in a harmful way. So the information officer should be able to protect this sensitive information.

Keywords: Hospital Administration, Security, Information, Health, Healthcare

INTRODUCTION

Information security is the process of protecting the availability, privacy, and integrity of data. While the term often describes measures and methods of increasing computer security, it also refers to the protection of any type of important data, such as personal diaries or the classified plot details of an upcoming book. No security system is foolproof, but taking basic and practical steps to protect data is critical for good information security. Unauthorised access to the information on computer or portable storage devices can be carried out remotely, if the 'intruder' is able to read or modify your data over the Internet; or physically, if he manages to get hold of your hardware. Encrypting information is a bit like keeping it in a locked safe. Only those who have a key or know the lock's combination (an encryption key or password, in this case) can access it. The analogy is particularly appropriate for VeraCrypt and tools like it, which create secure containers called 'encrypted volumes' rather than simply protecting one file at a time. You can put a large number of files into an encrypted volume, but these tools will not protect anything that is stored elsewhere on your computer or USB memory stick. Storing confidential data can be a risk for you and for the people you work with. Encryption reduces this risk but does not eliminate it. The first step to protecting sensitive information is to reduce how much of it you keep around. Unless you have a good reason to store a particular file, or a particular category of information within a file, you should simply delete it (Protect the Sensitive File on Your Computer https://securityinabox.org/en/guide/secure-file-storage/ 19.09.2017).

Password Protection

Using passwords is one of the most basic methods of improving information security. This measure reduces the number of people who have easy access to the information, since only those with approved codes can reach it. Unfortunately, passwords are not foolproof, and hacking programs can run through millions of possible codes in just seconds. Passwords can also be breached through carelessness, such as by leaving a public computer logged into an account or using a too simple code, like "password" or "1234."

To make access as secure as possible, users should create passwords that use a mix of upper and lowercase letters, numbers, and symbols, and avoid easily guessed combinations such as birthdays or family names. People should not write down passwords on papers left near the computer, and should use different passwords for each account. For better security, a computer user may want to consider switching to a new password every few months.

Antivirus and Malware Protection

One way that hackers gain access to secure information is through malware, which includes computer viruses, spyware, worms, and other programs. These pieces of code are installed on computers to steal information, limit usability, record user actions, or destroy data. Using strong antivirus software is one of the best ways of improving information security. Antivirus programs scan the system to check for any known malicious software, and most will warn the user if he or she is on a webpage that contains a potential virus. Most programs will also perform a scan of the entire system on command, identifying and destroying any harmful objects.

Most operating systems include a basic antivirus program that will help protect the computer to some degree. The most secure programs are typically those available for a monthly subscription or one-time fee, and which can be downloaded online or purchased in a store. Antivirus software can also be downloaded for free online, although these programs may offer fewer features and less protection than paid versions.

Even the best antivirus programs usually need to be updated regularly to keep up with the new malware, and most software will alert the user when a new update is available for downloading. Users must be aware of the name and contact method of each anti-virus program they own, however, as some viruses will pose as security programs in order to get an unsuspecting user to download and install more malware. Running a full computer scan on a weekly basis is a good way to weed out potentially malicious programs.

Firewalls

A firewall helps maintain computer information security by preventing unauthorized access to a network. There are several ways to do this, including by limiting the types of data allowed in and out of the network, re-routing network information through a proxy server to hide the real address of the computer, or by monitoring the characteristics of the data to determine if it's trustworthy. In essence, firewalls filter the information that passes through them, only allowing authorized content in. Specific websites, protocols (like File Transfer Protocol or FTP), and even words can be blocked from coming in, as can outside access to computers within the firewall.

Most computer operating systems include a pre-installed firewall program, but independent programs can also be purchased for additional security options. Together with an antivirus package, firewalls significantly increase information security by reducing the chance that a hacker will gain access to private data. Without a firewall, secure data is more vulnerable to attack.

Codes and Cyphers

Encoding data is one of the oldest ways of securing written information. Governments and military organizations often use encryption systems to ensure that secret messages will be unreadable if they are intercepted by the wrong person. Encryption methods can include simple substitution codes, like switching each letter for a corresponding number, or more complex systems that require complicated algorithms for decryption. As long as the code method is kept secret, encryption can be a good basic method of information security.

On computers systems, there are a number of ways to encrypt data to make it more secure. With a symmetric key system, only the sender and the receiver have the code that allows the data to be read. Public or asymmetric key encryption involves using two keys — one that is publicly available so that anyone can encrypt data with it, and one that is private, so only the person with that key can read the data that has been encoded. Secure socket layers use digital certificates, which confirm that the connected computers are who they say they are, and both symmetric and asymmetric keys to encrypt the information being passed between computers.

Legal Liability

Businesses and industries can also maintain information security by using privacy laws. Workers at a company that handles secure data may be required to sign non-disclosure agreements (NDAs), which forbid them from revealing or discussing any classified topics. If an employee attempts to give or sell secrets to a competitor or other unapproved source, the company can use the NDA as grounds for legal proceedings. The use of liability laws can help companies preserve their trademarks, internal processes, and research with some degree of reliability.

Training and Common Sense

One of the greatest dangers to computer data security is human error or ignorance. Those responsible for using or running a computer network must be carefully trained in order to avoid accidentally opening the system to hackers. In the workplace, creating a training program that includes information on existing security measures as well as permitted and prohibited computer usage can reduce breaches in internal security. Family members on a home network should be taught about running virus scans, identifying potential Internet threats, and protecting personal information online.

In business and personal behavior, the importance of maintaining information security through caution and common sense cannot be understated. A person who gives out personal information, such as a home address or telephone number, without considering the consequences may quickly find himself the victim of scams, spam, and identity theft. Likewise, a business that doesn't establish a strong chain of command for keeping data secure, or provides inadequate security training for workers, creates an unstable security system. By taking the time to ensure that data is handed out carefully and to reputable sources, the risk of a security breach can be significantly reduced. (Wisegeek http://www.wisegeek.org/what-is-information-security.htm 4.09.2017).

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules establish Federal requirements for keeping your health information secure. The HIPAA Privacy Rule generally requires health care providers and health plans to safeguard your health information. This requirement applies to both paper and electronic records. The HIPAA Security Rule more specifically details the steps your health care providers and others must take to keep your electronic protected health information secure.

Is all of my health information protected by HIPAA?

Privacy protections apply to your "individually identifiable health information," which means:

- Information that relates to your past, present, or future physical or mental health or condition; to the provision of health care to you; or to past, present, or future payment for the provision of health care to you.
- Information that identifies you or for which there is a reasonable basis to believe it can be used to identify you.

This information can include:

- Information your doctors, nurses, and other health care providers put in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer's computer system
- Billing information about you at your clinic
- Information used by companies or individuals that provide data, billing, or other services to doctors, hospitals, health insurers, and other health care organizations. This includes computer and data services providers, accountants, and other professional services firms.

When this information is held by an individual or organization that must follow HIPAA, it is called "protected health information."

The HIPAA Security Rule protections apply to electronic protected health information.

There are organizations that may have health information about you but do not have to follow the HIPAA Rules. For example, life insurers, employers, and workers' compensation carriers are not required to follow these Rules. However, privacy protections may be required through other laws they have to follow. The same is true for many schools and school districts, State agencies such as child protective service agencies, law enforcement agencies, and municipal offices.

How is my health information protected by HIPAA?

The people and organizations required to follow the HIPAA Privacy and Security Rules must:

- Follow the Rules about who can look at, receive, and share your health information
- Reasonably limit uses and sharing to the minimum necessary amount needed to accomplish their intended purpose. However, providers may disclose more than the minimum necessary when they are sharing information for treatment purposes.
- Have agreements in place with their service providers to ensure that they only use and share your health information according to the law

- Have procedures in place to limit who can access your health information as well as implement training programs for employees about how to protect your health information
- Put in place administrative, technical, and physical safeguards to protect your health information

What are some of the technical safeguards my providers use to protect my health information when it is stored in an electronic health record?

The HIPAA Security Rule requires providers to assess the security of their electronic health record systems. The Rule sets technical safeguards for protecting electronic health records against the risks that are identified in the assessment. Some of the steps that may be taken to reduce the risks include:

- Access controls such as passwords or PIN numbers that limit access to your information to authorized individuals, like your doctors or nurses
- Encryption of your information, which means your health information cannot be read or understood except by someone who can "decrypt" it, using a "key" made available only to authorized individuals
- Audit trails, which record who accessed your information, what changes were made, and when they were made, provide an additional layer of security
- Workstation security, which ensures that computer terminals that can access your health records cannot be used by unauthorized persons (Health IT Government https://www.healthit.gov/patients-families/your-health-information-security 2016)

Ways to improve the security

1. Eliminate shared accounts and their security risks. It is common practice for physicians and nurses to use shared accounts with one set of credentials for everyone. This is especially common in emergency rooms where employees use one PC to access vital information. To avoid spending valuable time logging into Windows and launching applications, one generic user account is often used, which is not secure as users can gain access to virtually any information on the machine. This also makes it difficult when it comes time for compliance audits. To alleviate this issue, physicians and nurses will need their own credentials for each application, but requiring them to remember all new credentials for each of the applications proves difficult. Also, logging in and out is a time consuming process. However, a single sign on application can ease this process and requires employees to only remember one set of credentials, making the process of eliminating shared accounts easy. Combining this with a smartcard is even more efficient. Once a user presents the smartcard to the reader, it is

recognized by the SSO software and the user is automatically logged in and the right applications are launched.

2. Keep employees from writing down passwords. Hospitals ideally should implement strong and complex passwords because of audit requirements, but implementing complex passwords has major consequences for end users. Often, if users need to remember several different and complex passwords, which also need to be changed regularly, they will write them down and store them somewhere. This makes the applications and systems insecure as people can easily view the credentials. With a single sign on solution, physicians and nurses will not need to write down their credentials as they will only need to remember one combination of username and password. This will eliminate this security risk and give hospitals the opportunity to easily implement complex passwords.

3. Give employees correct access rights. To ensure security of the network and information in a hospital, employees need to be given the correct security permissions based on their job roles. Ensuring that employees have the proper access rights greatly improves security. Doing so requires setting controls that can take the IT department months to implement. However, using a role based access control solution can assist with this process. They help the IT department easily populate the RBAC matrix and provide a simple overview of network resources available to an employee based on their position or access clearance.

4. Implement automatic user provisioning. Often, when employees leave employment at a hospital, the IT staff is not notified right away, and the employee's accounts are left open, allowing them the ability to access confidential information. This leaves the systems and information vulnerable and can have serious consequences. With an automated account management solution in place, the IT department can quickly and easily disable accounts as soon as an employee leaves to ensure security and compliance with audit standards.

5. Store information on user access. With a single sign on solution, information can be stored about who is logging into each application and what they are doing. This allows the IT department to easily review who has access to what and if their applications and systems are secure. This also allows them to comply with audit standards (Dean Wiech, U.S. Managing Director).

CONCLUSION

Vulnerabilities and intrusions pose risks for every hospital and its reputation. While there are significant benefits for care delivery and organizational efficiency from the expanded use of networked technology, Internet-enabled medical devices and electronic databases for clinical, financial and administrative operations, networked technology and greater connectivity also increase exposure to possible cybersecurity threats that require hospitals to evaluate and manage new risks. Hospitals can prepare and manage such risks by viewing cybersecurity not as a novel issue but rather by making it part of the hospital's existing governance, risk management and business continuity framework. Hospitals also will want to ensure that the approach they adopted remains flexible and resilient to address threats that are likely to be constantly evolving and multi-pronged (American Hospital Association). Data protection is important not only for the image of the hospital but also for the health and life of people, not just for their property and finances (the misuse of information from the hospital may be multidirectional).

In order to improve the security of information in healthcare establishments it is necessary to train the staff with the rules for the use of channels for transmission of information. It is also necessary to hire suitable people as well as companies that are able to keep systems in line with standards.

REFERENCES

AHA http://www.aha.org/advocacy-issues/cybersecurity/cybersecurity.shtml 04.09.2017

Dean Wiech, U.S. Managing Director, Tools4ever http://www.beckershospitalreview.com/healthcare-information technology/5ways-hospitals-can-improve-information-security.html 4.9.2017

Health IT Government https://www.healthit.gov/patients-families/your-health-information-security

Protect the Sensitive File on Your Computer https://securityinabox.org/en/guide/secure-file-storage/ 19.09.2017)

Wisegeek http://www.wisegeek.org/what-is-information-security.html 4.09.2017