11 Ways to Protect Your Hospital from Cyberattack

When health care providers think of viruses, it's rarely in a digital context. That doesn't make computer viruses any less harmful. Unfortunately, given the rise of cyberattacks on health care systems it's no longer "if" your system will suffer attack, but "when." Utilize this checklist when evaluating your hospital's cybersecurity efforts:

1

Establish a Security Culture

Frequent, ongoing education and training help to raise people's awareness about threats and vulnerabilities that can jeopardize the information they work with on a daily basis. Hospitals must instill a security culture among staff to the point that it becomes as second nature as maintaining sanitary practices.

2

Protect Mobile Devices

It is imperative employees take care to prevent data loss, either as a result of unauthorized viewing, unsecured wireless transmission, or stolen devices.

3

Maintain Good Computer Habits

IT staff must be careful to configure and maintain computer hardware and software to the degree that it's safe from harm. This includes removing any software that is not mission critical, updating software to the latest versions, and performing routine maintenance.

4

Use a Firewall

Unless a facility disconnects its EHR system from the Internet entirely, there should be a firewall surrounding it to protect against intrusions and threats from outside sources.

5

Install and Maintain Antivirus Software

Just as a firewall protects a network from intrusion, antivirus software detects and destroys malware. The anti-virus software can be thought of as infection control while the firewall has the role of disease prevention.

SCP HEALTH

6

Plan for the Unexpected

Two ways to protect against loss is by creating backups and having a recovery plan. Creating backups should be a daily or weekly routine. Recovery planning is necessary so when an emergency occurs, data restoration can take place quicker and more efficiently, following a prescribed process.

7

Control Access to Protected Health Information

Not every staff member needs the same level of access to sensitive information. Set permissions to restrict access using an “access control system” to assign user rights and permissions.

8

Use Strong Passwords and Change Them Regularly

Passwords are the first line of defense in preventing unauthorized access. A strong password could slow a hacker down long enough to discourage further attempts. Strong passwords consist of at least eight characters (the longer, the better), a combination of upper case and lower case letters, one number, and at least one special character, such as a punctuation mark.

9

Limit Network Access

The increase in cyberattacks means that the days of BYOD (bring your own device) to work are over. If not, it certainly means the hospital should not allow personal devices to access its network. Also, don’t allow staff to download software without explicit permission and oversight by IT staff.

10

Control Physical Access

The most common way electronic PHI is compromised is through the loss of devices, including: portable storage media (e.g., thumb or flash drives, CDs, or DVDs), laptops, handhelds, desktop computers, and even hard drives taken out of machines, lost and stolen backup tapes, and entire network servers.

Securing devices physically is a matter of grave importance. This included storing them in locked rooms, managing physical keys, and restriciting staff’s ability to remove devices from a secure area.

11

Implement a Tiered Approach

A tiered approach is a must for any technologist focused on securing a given environment. Long gone are the days where one security point product or appliance will meet all of the different security challenges hospitals are exposed to. Deploying multilayer firewalls or spam filters at the network edge and using multiple vendors can help reduce vulnerability.

While there is no way to keep cyberattacks from happening, following these 11 steps can help make your network safer and help protect medical records and other sensitive information. And if there is one other recommendation hospitals should heed, it’s to take action now and not wait until after a security breach occurs.

SCP HEALTH

888-902-3627 Business_Development@scp-health.com

scp-health.com