Top 10 Tips for Cybersecurity in Health Care

1. Establish a Security Culture

2. Protect Mobile Devices

3. Maintain Good Computer Habits

4. Use a Firewall

5. Install and Maintain Anti-Virus Software

6. Plan for the Unexpected

7. Control Access to Protected Health Information

8. Use Strong Passwords and Change Them Regularly

9. Limit Network Access

10. Control Physical Access

1. Establish a Security Culture

Security professionals are unanimous: The weakest link in any computer system is the user.

Researchers who study the psychology and sociology of Information Technology (IT) users have demonstrated time and again how very difficult it is to raise people's awareness about threats and vulnerabilities that can jeopardize the information they work with daily. The tips in this document describe some ways to reduce the risk, decreasing the likelihood that patients' personal health information will be exposed to unauthorized disclosure, alteration, and destruction or denial of access. But none of these measures can be effective unless the health care practice is willing and able to implement them, to enforce policies that require these safeguards to be used, and to effectively and proactively train all users so that they are sensitized to the importance of information security. In short, each health care practice must instill and support a security-minded organizational culture.

One of the most challenging aspects of instilling a security focus among users is overcoming the perception that "it can't happen to me." People, regardless of their level of education or IT sophistication, are alike in believing that they "will never succumb to sloppy practices or place patient information at risk. That only happens to other people."

The checklists included in this document are one proven way to overcome the human blind spot with respect to information security. By following a set of prescribed practices and checking them each time, at least some of the errors due to overconfidence can be avoided. But checklists alone are not enough. It is incumbent on any organization where lives are at stake to support proper information security through establishing a culture of security. Every person in the organization must subscribe to a shared vision of information security so that habits and practices are automatic.

Security practices must be built in, not bolted on.

No checklist can adequately describe all that must be done to establish an organization's security culture, but there are some obvious steps that must be taken:

- Education and training must be frequent and ongoing.
- Those who manage and direct the work of others must set a good example and resist the temptation to indulge in exceptionalism.
- Accountability and taking responsibility for information security must be among the organization's core values.

Protecting patients through good information security practices should be as second nature to the health care organization as sanitary practices.

2. Protect Mobile Devices

Mobile devices — laptop computers, handhelds, smartphones, portable storage media — have opened a world of opportunities to untether Electronic Health Records (EHRs) from the desktop. But these opportunities also present threats to information privacy and security. Some of these threats overlap those of the desktop world, but others are unique to mobile devices.

- Because of their mobility, these devices are easy to lose and vulnerable to theft.
- Mobile devices are more likely than stationary ones to be exposed to electromagnetic interference, especially from other medical devices. This interference can corrupt the information stored on a mobile device.
- Because mobile devices may be used in places where the device can be seen by others, extra care must be taken by the user to prevent unauthorized viewing of the electronic health information displayed on a laptop or handheld device.
- Not all mobile devices are equipped with strong authentication and access controls. Extra steps may be necessary to secure mobile devices from unauthorized use. Laptops should have password protection similar to the examples in Tip 8. Many handheld devices can be configured with password protection, and these protections should be enabled when available. If password protection is not provided, additional steps must be taken to protect electronic health information on the handheld, including extra precaution over the physical control of the device.
- Laptop computers and handheld devices are often used to transmit and receive data wirelessly. These wireless communications must be protected from eavesdropping and interception (Tip 9 describes wireless network protection). Cybersecurity experts recommend not transmitting electronic health information across public networks without encryption.

Transporting data with mobile devices is inherently risky. There must be an overriding justification for this practice that rises above mere convenience. The U.S. Department of Health and Human Services (HHS) has developed guidance on the risks and possible mitigation strategies for remote use of and access to electronic health information.[1]

Where it is absolutely necessary to commit electronic health information to a mobile device, cybersecurity experts recommend that the data be **encrypted**. Mobile devices that cannot support encryption should not be used. Encrypted devices are readily obtainable at a modest cost — much less than the cost of mitigating a data breach.

If it is absolutely necessary to take a laptop containing electronic health information out of a secure area, you should protect the information on the laptop's hard drive through encryption.

[1] http://healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

Policies specifying the circumstances under which devices may be removed from the facility are very important, and all due care must be taken in developing and enforcing these policies. The primary goal is to protect the patient's information, so considerations of convenience or custom (e.g., working from home) must be considered in that light.

But I Need to Work at Home

In today's increasingly mobile world, it is certainly tempting to use mobile technology to break away from the office and perform work from the comfort of home. Those who have responsibility for protecting patient information must recognize that this responsibility does not end at the office door. Good privacy and security practices must always be followed.

Download Mobile Device Checklist[2]

3. Maintain Good Computer Habits

The medical practitioner is familiar with the importance of healthy habits to maintain good health and reduce the risk of infection and disease. The same is true for IT systems, including EHR systems — they must be properly maintained so that they will continue to function properly and reliably in a manner that respects the importance and the sensitive nature of the information stored within them. As with any health regimen, simple measures go a long way.

Configuration Management

New computers and software packages are delivered with a dizzying array of options and little guidance on how to configure them so that the system is secure. In the face of this complexity, it can be difficult to know what options to permit and which to turn off. While a publication of this length cannot go into detail on this topic, there are some rules of thumb:

- Uninstall any software application that is not essential to running the practice (e.g., games, instant message clients, photo-sharing tools). If the purpose of a software application is not obvious, look at the software company's web site to learn more about the application's purposes and uses. Also check with the EHR developer to see if the software is critical to the EHR's function.
- Do not simply accept defaults or "standard" configurations when installing software. Step through each option, understand the choices, and obtain technical assistance where necessary.
- Find out whether the EHR vendor maintains an open connection to the installed software (a "back door") in order to provide updates and support. If so, ensure a secure connection at the firewall and request that this access be disabled when not in use.

[2] http://healthit.gov/sites/default/files/Mobile_Device_Checklist.pdf

- Disable remote file sharing and remote printing within the operating system configuration. Allowing these could result in the accidental sharing or printing of files to locations where unauthorized individuals could access them.

Software Maintenance

Most software requires periodic updating to keep it secure and to add features. Vendors may send out updates in various ways, including automated downloads and customer-requested downloads.

Keeping software up-to-date is critical to maintaining a secure system, since many of these updates address newly found vulnerabilities in the product. In larger enterprises, this "patching" can be a daily task, where multiple vendors may issue frequent updates. In the small practice, there may not be the resources to continually monitor for new updates and apply them in good time. Small practices may instead wish to automate updates to occur weekly (e.g., use Microsoft Windows Automatic Update). However, practices should monitor for critical and urgent patches and updates that require immediate attention. Messages from vendors regarding these patches and updates should be monitored and acted upon as soon as possible.

Operating System (OS) Maintenance

Over time, an operational system tends to accumulate outdated information and settings unless regular maintenance is performed. Just as medical supplies have to be monitored for their expiration dates, material that is out-of-date on a computer system must be dealt with. Things to check include:

- User accounts for former employees are appropriately and timely disabled. If an employee is to be involuntarily terminated, disable access to the account before the notice of termination is served.
- Computers and any other devices, such as copy machines, that have had data stored on them are "sanitized" before disposal. Even if all the data on a hard drive has been deleted, it can still be recovered with commonly available tools. To avoid the possibility of an unintended data breach, follow the guidelines for disposal found in the National Institute of Standards and Technology (NIST) Special Publication 800-88 "Guidelines for Media Sanitation."[3]
- Old data files are archived for storage if needed, or cleaned off the system if not needed, subject to applicable data retention requirements.
- Software that is no longer needed is fully uninstalled (including "trial" software and old versions of current software).

[3] http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

How do you know if staff members have downloaded programs they are not supposed to?

There are several commercial applications and services (e.g., anti-malware and anti-virus programs) that can be set up to report or even stop the download of rogue/unapproved software. They can conduct vulnerability and configuration scans, and some applications/services can conduct general security audits as well (e.g., other technical, administrative, and physical safeguards). Work with your IT team or other resources to perform malware, vulnerability, configuration, and other security audits on a regular basis.

Download Maintenance Checklist[4]

4. Use a Firewall

Unless a small practice uses an EHR system that is totally disconnected from the Internet, it should have a firewall to protect against intrusions and threats from outside sources. While anti-virus software will help to find and destroy malicious software that has already entered, a firewall's job is to prevent intruders from entering in the first place. In short, the anti-virus can be thought of as infection control while the firewall has the role of disease prevention.

A firewall can take the form of a software product or a hardware device. In either case, its job is to inspect all messages coming into the system from the outside (either from the Internet or from a local network) and decide, according to pre-determined criteria, whether the message should be allowed in.

Configuring a firewall can be technically complicated, and hardware firewalls should be configured by trained technical personnel. Software firewalls, on the other hand, are often pre-configured with common settings that tend to be useful in many situations. Software firewalls are included with some popular operating systems, providing protection at the installation stage. Alternatively, separate firewall software is widely available from computer security vendors, including most of the suppliers of anti-virus software. Both types of firewall software normally provide technical support and configuration guidance to enable successful configuration by users without technical expertise.

When should a hardware firewall be used?

Large practices that use a Local Area Network (LAN) should consider a hardware firewall. A hardware firewall sits between the LAN and the Internet, providing centralized management of firewall settings. This increases the security of the LAN, since it ensures that the firewall settings are uniform for all users.

[4] http://healthit.gov/sites/default/files/Maintenance_Checklist.pdf

If a hardware firewall is used, it should be configured, monitored, and maintained by a specialist in this subject.

Download Firewall Checklist[5]

5. Install and Maintain Anti-Virus Software

The primary way that attackers compromise computers in the small office is through viruses and similar code that exploits vulnerabilities on the machine. These vulnerabilities are ubiquitous due to the nature of the computing environment. Even a computer that has all of the latest security updates to its operating system and applications may still be at risk because of previously undetected flaws. In addition, computers can become infected by seemingly innocent outside sources such as CDs, email, flash drives, and web downloads. Therefore, it is important to use a product that provides continuously updated protection. Anti-virus software is widely available, well-tested to be reliable, and costs relatively little.

After implementation of EHRs, it is important to keep anti-virus software up-to-date. Anti-virus products require regular updates from the vendor in order to protect against the newest computer viruses and malware. Most anti-virus software automatically generates reminders about these updates, and many are configurable to allow for automated updating.

Without anti-virus software, data may be stolen, destroyed, or defaced, and attackers could take control of the machine.

How can users recognize a computer virus infection?

Some typical symptoms of an infected computer include:

- System will not start normally (e.g., "blue screen of death")
- System repeatedly crashes for no obvious reason
- Internet browser goes to unwanted web pages
- Anti-virus software does not appear to be working
- Many unwanted advertisements pop up on the screen
- The user cannot control the mouse/pointer

Download Anti-Virus Checklist[6]

[5] http://healthit.gov/sites/default/files/Firewall_Checklist.pdf
[6] http://healthit.gov/sites/default/files/Anti-Virus_Checklist.pdf

6. Plan for the Unexpected

Sooner or later, the unexpected will happen. Fire, flood, hurricane, earthquake, and other natural or man-made disasters can strike at any time. Important health care records and other vital assets must be protected against loss from these events. There are two key parts to this practice: creating backups and having a sound recovery plan.

In the world of business, creating a backup is routine. In the small practice, however, it may be that the staff members are only familiar with a home computing environment, where backups are rarely considered until a crash happens, by which time it is too late. From the first day a new EHR is functioning in a practice, the information must be backed up regularly and reliably. A reliable backup is one that can be counted on in an emergency, so it is important not only that all the data be correctly captured, but that it can quickly and accurately be restored. Backup media must be tested regularly for their ability to restore properly.

Whatever medium is used to hold the backup (e.g., magnetic tape, CD, DVD, removable hard drive), it must be stored safely so that it cannot be wiped out by the same disaster that befalls the main system. Depending on the local geography or type of risk, this could mean that backups should be stored many miles away. One emerging option for backup storage is cloud computing, which may be a viable option for many, since it involves no hardware investment and little technical expertise. However, cloud backup must be selected with care. The backed-up data must be as secure as the original.

Critical files can be manually copied onto backup media, although this can be tedious and potentially error-prone. If possible, an automated backup method should be used.

Some types of backup media are reusable, such as magnetic tape and removable hard drives. These media can wear out over time and after multiple backup cycles. It is especially important to test them for reliable restore operations as they age.

Storage of backup media must be protected with the same type of access controls as described in Tips 7 and 10. The Contingency Planning Safety Assurance Factors for EHR Resilience (SAFER) Guide[7] identifies recommended safety practices associated with planned or unplanned EHR unavailability.

Recovery planning must be done so that when an emergency occurs, there is a clear procedure in place. In a disaster, it is possible that health care practices will be called upon to supply medical records and information rapidly. The practice must be prepared to access their backups and restore functionality, which requires knowledge about what data was backed up, when the backups were done (timeframe and frequency), where the backups are stored, and what types of equipment are

[7] http://healthit.gov/safer/guide/sg003

needed to restore them. If possible, this information must be placed for safekeeping at a remote location where someone has responsibility for producing it in the event of emergency.

Is it OK to store my backup media at home?

A fireproof, permanently installed home safe, which only the health care provider knows the combination for, may be the most feasible choice for many practices to store backup media. This would not place the backup out of the danger zone of a widespread disaster (earthquake, hurricane, nuclear), but it would provide some safety against local emergencies such as fire and flood. Fireproof portable boxes or safes where non-staff have the combination are inadequate.

Download Backup and Recovery Checklist[8]

7. Control Access to Protected Health Information

To minimize the risk to electronic health information when effectively setting up EHR systems, Tip 8 discusses the importance of passwords. The password, however, is only half of what makes up a computer user's credentials. The other half is the user's identity, or user name. In most computer systems, these credentials (user name and password) are used as part of an **access control** system in which users are assigned certain rights to access the data within. This access control system might be part of an operating system (e.g., Windows) or built into a particular application (e.g., an e-prescribing module); often both are true. In any case, configure your EHR implementation to grant electronic health information access **only to people with a "need to know**."

For many situations in small practices, setting file access **permissions** may be done manually, using an **access control list**. This can only be done by someone with authorized rights to the system. Prior to setting these permissions, it is important to identify which files should be accessible to which staff members.

Additional access controls that may be configured include **role-based access control**, in which a staff member's role within the practice (e.g., physician, nurse, billing specialist) determines what information may be accessed. In this case, care must be taken to assign staff to the correct roles and then to set the access permissions for each role correctly with respect to the need to know.

The combination of regulations and the varieties of access control possibilities make this one of the more complex processes involved in setting up an EHR system in the small practice.

[8] http://healthit.gov/sites/default/files/Backup_and_Recovery_Checklist.pdf

What if electronic health information is accessed without permission?

Under certain circumstances, such an incident is considered a breach that has to be reported to HHS (and/or a state agency if there is such a requirement in the state's law). Having good access controls and knowledge of who has viewed or used information (i.e., access logs) can help to prevent or detect these data breaches.

Download Access Control Checklist[9]

8. Use Strong Passwords and Change Them Regularly

General Information

Passwords are the first line of defense in preventing unauthorized access to any computer. Regardless of type or operating system, a password should be required to log in. Although a strong password will not prevent attackers from trying to gain access, it can slow them down and discourage them. In addition, strong passwords, combined with effective access controls, help to prevent casual misuse (e.g., staff members pursuing their personal curiosity about a case even though they have no legitimate need for the information).

Strong passwords are ones that are not easily guessed. Since attackers may use automated methods to try to guess a password, it is important to choose a password that does not have characteristics that could make it vulnerable.

Strong passwords should **not include**:

- Words found in the dictionary, even if they are slightly altered (e.g., replacing a letter with a number)
- Personal information such as birth date; names of self, family members, or pets; social security number; or anything else that could easily be learned by others. Remember: If a piece of information is on a social networking site, it should never be used in a password.

Below are some examples of strong password characteristics:

- At least eight characters in length (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] http://healthit.gov/sites/default/files/Access_Control_Checklist.pdf

Finally, systems should be configured so that passwords must be changed on a regular basis. While this may be inconvenient for users, it also reduces some of the risk that a system will be easily broken into with a stolen password.

Passwords and Strong Authentication

Strong, or multi-factor, authentication combines multiple different authentication methods, resulting in stronger security. In addition to a user name and password, another authentication method is used (e.g., a smartcard, key fob, or fingerprint or iris scan).

Under federal regulations permitting e-prescribing of controlled substances, multi-factor authentication must be used.

What about forgotten passwords?

Anyone can forget a password, especially if the password is long. To discourage people from writing down their passwords and leaving them in unsecured locations, plan for password resetting. This could involve 1) allowing two different staff members to be authorized to reset passwords; or 2) selecting a product that has built-in password reset capabilities.

Download Password Checklist[10]

9. Limit Network Access

Ease of use and flexibility make contemporary networking tools very appealing. Web 2.0 technologies like peer-to-peer file sharing and instant messaging are popular and widely used. Wireless routing is a quick and easy way to set up broadband capability within a home or office. However, because of the sensitivity of health care information and the fact that it is protected by law, tools that might allow outsiders to gain access to a health care practice's network must be used with extreme caution.

Wireless routers that allow a single incoming Internet line to be used by multiple computers are readily available for less than $100. For the small practice that intends to rely on wireless networking, special precautions are in order. Unless the wireless router is secured, its signal can be picked up from some distance away, including, for example, the building's parking lot, other offices in the same building, or even nearby homes. Since electronic health information flowing over the wireless network must be protected by law, it is crucial to secure the wireless signal so that only those who are permitted to access the information can pick up the signal. Wireless routers must be set up to operate only in **encrypted mode.**

[10] http://healthit.gov/sites/default/files/Password_Checklist.pdf

Devices brought into the practice by visitors should not be permitted access to the network, since it is unlikely that such devices can be fully vetted for security on short notice. Setting up a network to safely permit guest access is expensive and time-consuming, so the best defense is to prohibit casual access. When a wireless network is configured, each legitimate device must be identified to the router, and only then can the device be permitted access.

Peer-to-peer applications, such as file sharing and instant messaging, can expose the connected devices to security threats and vulnerabilities, including permitting unauthorized access to the devices on which they are installed. Check to make sure peer-to-peer applications have not been installed without explicit review and approval. It is not sufficient to just turn these programs off or uninstall them. A machine containing peer-to-peer applications may have exploitable bits of code that are not removed even when the programs are removed.

A good policy is to prohibit staff from installing software without prior approval.

Download Network Access Checklist[11]

10. Control Physical Access

Not only must assets like files and information be secured; the devices themselves that make up an EHR system must also be safe from unauthorized access. The single most common way that electronic health information is compromised is through the loss of devices, whether this happens accidentally or through theft. Incidents reported to the Office for Civil Rights show that more than half of all these data loss cases consist of missing devices, including portable storage media (e.g., thumb or flash drives, CDs, or DVDs), laptops, handhelds, desktop computers, and even hard drives ripped out of machines, lost and stolen backup tapes, and entire network servers.

Should a data storage device disappear — no matter how well an office has taken care of its passwords, access control, and file permissions — it is still possible that a determined individual could access the information on it. Therefore, it is important to limit the chances that a device may be tampered with, lost, or stolen.

Securing devices and information physically should include policies limiting physical access, e.g., securing machines in locked rooms, managing physical keys, and restricting the ability to remove devices from a secure area.

Where should I place my server that stores electronic health information?

When considering where to locate a server containing electronic health information (such as within an EHR), two main factors should be considered: physical and environmental protection. Physical

[11] http://healthit.gov/sites/default/files/Network_Access_Checklist.pdf

protection should be focused on preventing unauthorized individuals from accessing the server (e.g., storing the server in a locked room accessible only to staff). Environmental protections should focus on protecting the server from fire, water, and other elements (e.g., never store a server in a restroom; instead store the server off the floor, away from water and windows, and in a temperature-regulated room).

Download Physical Access Checklist[12]

[12] http://healthit.gov/sites/default/files/Physical_Access_Checklist.pdf