V 1.0 November, 2010

CYBERSECURITY

The protection of data and systems in networks that connect to the Internet

10 Best Practices For The Small Healthcare Environment

GA-HITREC
720 Westview Dr, SW
Atlanta, GA 30310
Phone:404-752-1015
Toll Free - 877-658-1990
FAX: 404-756-5767
www.ga-hitrec.org

The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The material in this guide is designed to provide information regarding best practices and assistance to Regional Extension Center staff in the performance of technical support and implementation assistance. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein. This guide does not guarantee compliance with the applicable laws and each healthcare practice has different needs, risks and vulnerabilities. This guide should not be relied upon for any purpose and serves merely as a tool for consideration in combination with other resources pertinent to the individual practice.

This document is for duplex printing.

Table of Contents

This page intentionally left blank.

Background

Cybersecurity: The protection of data and systems in networks that connect to the Internet - 10 Best Practices for the Small Healthcare Environment

Good patient care means safe record-keeping practices. Never forget that the electronic health record (EHR) represents a unique and valuable human being: it is not just a collection of data that you are guarding. It is a life.

Stage 1 Meaningful Use criteria make it virtually certain that eligible providers will have to have an Internet connection. To exchange patient data, submit claims electronically, generate electronic records for patients' requests, or e-prescribe, an Internet connection is a necessity, not an option. To protect the *confidentiality, integrity, and availability* of electronic health record systems, regardless of how they are delivered; whether installed in a physician's office, accessed over the Internet, basic **cybersecurity** practices are needed.

The U.S. Department of Health and Human Service (HHS), through the Office of the National Coordinator for Health Information Technology (ONC) is providing this guide as a first take on the key security points to keep in mind when protecting EHRs.

Depending on the configuration of the EHR, some of these best practices may be more applicable than others. ONC's Regional Extension Centers (RECs) can be of assistance in determining which are applicable and which are not.

We also remind small practices that the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules provides federal protections for protected health information (PHI) held by covered entities and gives patients an array of rights with respect to that information. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information, including the requirement under the HIPAA Security Rule to perform a risk analysis as part of their security management processes. It is important to understand that the following cybersecurity practices are not intended to provide guidance regarding how to comply with HIPAA; rather, they are a first step to the effective setup of new EHR systems in a way that minimizes the risk to health information maintained in EHRs. Guidance about how to comply with the HIPAA Privacy and Security Rules can be found on the HHS Office for Civil Rights (OCR) website at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.

How to Use This Guide

This guide contains explanations for each of the ten identified best practices, as well as checklists to support healthcare practices validating that they are meeting the basic requirements outlined in each section. The document has been formatted for ease of use. Simply print out the guide in a duplex (double-sided) format. The checklists, numbered by section, are at the end of the document and can be removed to be used as standalone pages. In electronic form, each checklist is linked back to the section that references it.

The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The material in this guide is designed to provide information regarding best practices and assistance to Regional Extension Center staff in the performance of technical support and implementation assistance. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein. This guide does not guarantee compliance with the applicable laws and each healthcare practice has different needs, risks and vulnerabilities. This guide should not be relied upon for any purpose and serves merely as a tool for consideration in combination with other resources pertinent to the individual practice.

Introduction

Why Should Healthcare Practices Worry About Security?

The Threat of Cyber Attacks: Most everyone has seen news reports of cyber attacks against, for example, nationwide utility infrastructures or the information networks of the Pentagon. Healthcare providers may believe that if they are small and low profile, they will escape the attentions of the "bad guys" who are running these attacks. Yet, every day there are new attacks aimed specifically at small to mid-size organizations for the very reason that they are low profile and less likely to have fully protected themselves. Criminals have been highly successful at penetrating these smaller organizations, carrying out their activities while their unfortunate victims are unaware until it is too late.

What is "cyber" security?

The protection of data and systems in networks that connect to the Internet.

This definition applies to any computer or other device that can transmit electronic health records to another device over a network connection, whether it uses the Internet or some other network.

It is vital to do as much as possible to protect sensitive health information in EHRs. The consequences of a successful cyber attack could be very serious, including loss of patient trust, violations of the Health Insurance Portability and Accountability Act (HIPAA), or even loss of life or of the practice itself. Real-world examples large and small abound. Barely a day goes by that the press does not have reports of the latest cyber-attacks.

Until now, relatively few healthcare practices have been targeted by these criminals. With increasing adoption of EHRs, many more practices will soon have new systems in place, which could increase the level of attacks.

Our Own Worst Enemy: Even though cyber attacks from hackers and other criminals grab a lot of headlines, research indicates that often times, well-meaning computer users can be their own worst enemies. Why? Because they fail to follow basic safety principles. This might be due to lack of training, time pressures, or any of a range of reasons. Yet, following these practices can sometimes be just as important and just as basic to patient safety as good hand-washing practice.

This document will discuss ten simple best practices that should be taken to reduce the most important threats to the safety of electronic health records. This core set of best practices was developed by a team of cybersecurity and healthcare subject matter experts to address the unique needs of the small healthcare practice. They are based on a compilation and distillation of cybersecurity best practices, particularly those developed under the auspices of the Information Security Alliance.

Practice 1: Use strong passwords and change them regularly

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 and do any work. Although a strong password will not prevent attackers from trying to gain access, it can slow them down and discourage all but the most determined. In addition, strong passwords, combined with effective access controls, help to prevent casual misuse, for example, 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, for example by replacing a letter with a number.
- Personal information such as birth date, names of self, or family, 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.

What about forgotten passwords?

Anyone can forget a password. The longer the password, the more likely this occurrence. To discourage people from writing down their passwords and leaving them in unsecured locations, plan for password recovery. This could involve allowing two different staff members to be authorized to add, delete and/or re-set passwords, storing passwords in a safe, or selecting a product that has built-in password recovery tools.

Strong passwords **should**:

- Be at least 8 characters in length
- Include a combination of upper case and lower case letters, at least one number and at least one special character, such as a punctuation mark

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 method is used. While a username is something you know and a password is something you know, multi-factor authentication also includes either something you have, like a smart card or a key-fob, or something that is part of who you are, such as a fingerprint or a scan of your iris.

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

Practice 2: 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 CD-ROMs, e-mail, flash drives, and web downloads. Therefore, it is important to use a product that provides continuously updated protection against these exploits. Anti-virus software is widely available, well-tested to be reliable, and costs relatively little.

After implementation it is important to keep anti-virus software up to date. Anti-virus products require regular updates from the vendor in order to protect from 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..

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 appears not to be working
- Many unwanted advertisements pop up on the screen
- The user cannot control the mouse/pointer

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

Practice 3: Use a Firewall

Unless a small practice uses an EHR system that is totally disconnected from the Internet[1], 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 determine, 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.

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

[1] An unlikely case, but theoretically possible.

Practice 4: Control Access to Protected Health Information

All health care providers, health plans, and health care clearinghouses that transmit health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA are "covered entities" and must comply with the HIPAA Privacy and Security Rules. The HIPAA Rules define "protected health information" (PHI) as all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Generally, "individually identifiable health information" is information that relates to an individual's health and that identifies an individual or for which there is a reasonable basis to believe can be used to identify an individual.

To minimize the risk to protected health information when effectively setting up EHR systems, Practice 1 discussed the importance of passwords. The password, however, is only one 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, an EHR implementation needs to be configured to grant access to PHI **only to people with a need to know it.** The need to know is narrowly defined, so EHR systems should be configured carefully to allow limitation of access in all but the smallest practices.

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 administrative rights to the system, which means that this individual must be fully trusted. Prior to setting these permissions, it is important to identify which files should be accessible to which staff members.

What if protected health information is accessed without permission?

If protected health information is accessed by a person not authorized to access it, then this could indicate a violation of both the HIPAA Privacy and Security Rules. Under certain circumstances, such an incident may have to be reported to HHS and/or a state agency as a **breach** of unsecured protected health information. 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.

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) 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 of setting up an EHR system in the small practice.

Practice 5: Control Physical Access

Not only must assets like files and information to be secured, the devices themselves that make up an EHR system must also be safe from unauthorized access. The single most common way that protected health information is compromised is through the loss of devices themselves, whether this happens through theft or accidentally. Incidents reported to HHS's 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, CD or DVD disks), 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 possibility of devices disappearing or being tampered with.

Securing devices and information physically should include policies limiting physical access, for example, 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 PHI?

When considering where to locate a server with EHR, PHI or other PII two main factors should be considered: physical and environmental protection. Physical protection should be focused on preventing unauthorized individuals from accessing the server (e.g. storing the server in 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).

Practice 6: 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 healthcare information and the fact that it is protected by law; tools that might allow outsiders to gain access to a healthcare practice's network must be used with extreme caution.

Wireless routers that allow a single incoming cable or DSL 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 PHI data 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. When a wireless router is used, it must be set up to operate only in **encrypted mode**[2].

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. In configuring a wireless network, each legitimate device must be identified to the router and only those devices 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 these and other 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..

Practice 7: 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 healthcare 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.

[2] Encryption modes are specified in IEEE standard 802.11i. This standard is commonly referenced on the packaging of wireless routers. The correct encryption modes are WPA2 or WPA, *not* WEP.

In the world of business, creating a backup is routine practice. 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 data 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 data (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 and must be stored according to HIPAA regulatory requirements.

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.

Is it OK to store my backup media at home?

A fireproof, permanently installed home safe, which only the healthcare 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.

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 described above in Practices 4 and 5.

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 healthcare 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 where the backups are stored, how they were prepared, and what types of equipment are needed to read 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.

Practice 8: 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 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 data 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 booklet 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, IM clients, photo sharing tools). If the purpose of a software application is not obvious, check with the EHR vendor and look it up by name on any of the several web sites that maintain databases of applications and their purpose.
- Do not simply accept defaults or "standard" configurations when installing software. Step through each option, understand the choices, and obtain technical assistance where necessary[3].
- 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, this connection must be well-secured at the firewall and its traffic monitored closely in case it is found by intruders.
- 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 view them.

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

There are several applications and services available commercially that perform **desktop audits**. These applications/services can be set up to report or even stop the download of rogue/unapproved software. Some of these also have other useful functions, like doing a general security audit. Product recommendations are beyond the scope of this guide, but a quick search on "software audit" will turn up many hits.

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, customer-requested downloads, and on portable media. 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.

[3] REC representatives are available to provide technical assistance, visit the ONC website for more information.

Operating 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, access to the account should be disabled before the notice of termination is served.
- Computers and any other devices, such as copying 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 NIST Special Publication 800-88 "*Guidelines for Media Sanitation*".
- 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).

Practice 9: Protect Mobile Devices

Mobile devices—laptop computers, handhelds, smart phones, portable storage media—have opened a world of opportunities to un-tether EHRs from the desktop. But these opportunities also present threats to information security and privacy. Some of these threats overlap those of the desktop world, but others are unique to mobile devices.

- Because of their very mobility, these devices are easy to lose and because they may be used in areas accessible to the public, they are very vulnerable to theft.
- Mobile devices are more likely than stationary ones to be exposed to electro-magnetic interference (EMI), especially from other medical devices, such as MRI machines. 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 PHI 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 that conforms to that described in Practice 1. Many handheld devices can be configured with password protection and this should be enabled when available. Where not available, additional steps must be taken to protect PHI on the handheld, including extra precaution over the physical control of the device.

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 data must recognize that this responsibility does not end at the office door and follow good security practices wherever they take people's PHI.

- Laptop computers and handheld devices are often used to transmit and receive data wirelessly. These wireless communications must be protected from intrusion (Practice 6 describes wireless network protection). PHI transmitted unencrypted across *public* networks (e.g. the Internet, public Wi-Fi services) can be done where the patient requests it and has been informed of the potential risks. Generally, however, PHI should not be transmitted without encryption across these *public* networks.

Transporting data with mobile devices is inherently risky. There must be an overriding justification for this practice that rises above mere convenience.

Where it is absolutely necessary to commit PHI to a mobile device, the data should be **encrypted**. Mobile devices that cannot support encryption should not be used. This includes the inexpensive memory sticks or thumb drives that are widely available and often given away by vendors. Encrypted versions of these 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 out of a secure area when the laptop contains patient data, the laptop's hard drive should be **encrypted.**

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. 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.

Practice 10: 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 users have demonstrated time and again how very difficult it is to raise peoples' awareness about threats and vulnerabilities that can jeopardize the information they work with daily. Practices 1-9 in this booklet describe some ways to reduce the risk, decreasing the likelihood that patients' personal health information will be exposed to unauthorized view. But none of these measures can be effective unless the healthcare 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 data security. In short, each healthcare 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. *They* will never place patient data at risk. That only happens to other people."

The checklists that follow are one proven way to overcome the human blind spot with respect to data security. By following a set of prescribed practices and checking them each time, at least some of the errors due to over-confidence 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 where data security is part of its very fabric. 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, including:

- Education and training must be frequent and on-going.
- 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 safety must be among the organization's core values.

Protecting patients through good data security practice should be as much second nature to the healthcare practice as disinfection is.

This page intentionally left blank.

Security Checklists

This page intentionally left blank.

Practice 1: Password Checklist

□ Policies are in place prescribing password practices for the organization.

□ All staff understand and agree to abide by password policies.

□ Each staff member has a unique username and password.

□ Passwords are not revealed or shared with others.

□ Passwords are not written down or displayed on screen.

□ Passwords are hard to guess, but easy to remember.

□ Passwords are changed routinely.

□ Passwords are not re-used.

□ Any default passwords that come with a product are changed during product installation.

□ Any devices or programs that allow optional password protection have password protection turned on and in use.

Strong passwords **should**:

- Be at least 8 characters in length
- Include a combination of upper case and lower case letters, at least one number and at least one special character, such as a punctuation mark
- Be changed often, at least quarterly.

This page intentionally left blank.

Practice 2: Anti-Virus Checklist

□ Policies are in place requiring use of anti-virus software.

□ All staff understand and agree that they shall not hinder the operation of anti-virus software.

□ All staff know how to recognize possible symptoms of viruses or malware on their computers.

□ All staff know what to do to avoid virus/malware infections.

□ Anti-virus software is installed and operating effectively on each computer in compliance with manufacturer recommendations.

□ Anti-virus software is set up to allow automatic updates from the manufacturer.

□ Anti-virus software is fully up-to-date according to manufacturer's standards.

□ Handheld or mobile devices that support anti-virus software have it installed and operating.

This page intentionally left blank.

Practice 3: Firewall Checklist

□ Policies are in place prescribing the use, configuration, and operation of firewalls and firewall logs.

□ All computers are protected by a properly configured firewall.

□ All staff understand and agree that they may not hinder the operation of firewalls.

This page intentionally left blank.

Practice 4: Access Control Checklist

□ Policies are in place prescribing access controls.

Example: “When an employee quits, his/her user account is disabled immediately”

□ Every user account can be positively tied to a currently authorized individual.

□ Users are only authorized to access information which they need to know to perform their duties.

□ All files have been set to restrict access only to authorized individuals.

□ All staff understand and agree to abide by access control policies.

□ Computers running healthcare-related systems are not available for other purposes.

This page intentionally left blank.

Practice 5: Physical Access Checklist

□ Policies are in place prescribing the physical safety and security of devices and devices.

□ All staff understand and agree to abide by physical access policies and procedures.

□ All devices containing PHI are inventoried and can be accounted for.

□ Computers are protected from environmental hazards.

□ Physical access to secure areas is limited to authorized individuals.

□ Computers running EHR systems are shielded from unauthorized viewing.

□ Equipment located in high-traffic or less secure areas is physically secured.

This page intentionally left blank.

Practice 6: Network Access Checklist

- □ Policies are in place prescribing network configuration and access.
- □ All staff understand and agree to abide by network use policy.
- □ Access to the network is restricted to authorized users and devices.
- □ Guest devices are prohibited from accessing networks containing PHI.
- □ Wireless networks use appropriate encryption.
- □ Computers contain no peer-to-peer applications.
- □ Public instant messaging services are not used.
- □ Private instant messaging services, where used, are secured appropriately.

This page intentionally left blank.

Practice 7: Backup and Recovery Checklist

□ Policies are in place prescribing backup and recovery procedures.

□ All staff understand the recovery plan and their duties during recovery.

□ System restore procedures are known to at least one trusted party outside the practice.

□ A copy of the recovery plan is safely stored off-site.

□ Files identified as critical are documented and listed in the backup configuration.

□ Backup schedule is timely and regular.

□ Every backup run is tested for its ability to restore the data accurately.

□ Backup media are physically secured.

□ Backup media stored offsite are encrypted.

□ Backup media are made unreadable before disposal.

□ Multiple backups are retained as a failsafe.

This page intentionally left blank.

Practice 8: Maintenance Checklist

□ Policies are in place prescribing EHR system maintenance procedures.

□ Staff with responsibilities for maintenance understand and agree to system maintenance policies and procedures.

□ Computers are free of unnecessary software and data files.

□ Remote file sharing and printing (including remote printing) are disabled.

□ Vendor remote maintenance connections are documented and fully secured.

□ Systems and applications are updated or patched regularly as recommended by the manufacturer.

This page intentionally left blank.

Practice 9: Mobile Devices Checklist

- □ Policies are in place prescribing use of mobile devices.
- □ All staff understand and agree to abide by mobile device policy and procedures.
- □ Mobile devices are configured to prevent unauthorized use.
- □ PHI on mobile devices is encrypted.
- □ Connections between authorized mobile devices and EHRs are encrypted.

This page intentionally left blank.

List of Acronyms

Acronym	Acronym Description
AES	Advanced Encryption System
CD	compact disc
CD-ROM	compact disc read-only-memory
DSL	digital subscriber line
DVD	digital video disk
EHR	electronic health record
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HITRC	Health Information Technology Research Center
IEEE	Institute of Electrical and Electronic Engineers
IM	instant message
LAN	local area network
NAT	network address translation
NIST	National Institute of Standards and Technology
ONC	Office of the National Coordinator for Health Information Technology
PC	personal computer
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PHI	protected health information
REC	Regional Extension Center
USB	Universal Serial Bus
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

References & Resources

Recognizing that this document is not intended to be and should not be construed as an exhaustive guide on protecting PHI, we have provided additional resources and references that have helped guide the creation of this document. These references and resources may be used to obtain additional detailed technical guidance to supplement this document. It should be recognized that due to the changing nature of the information security field, additional technical resources may exist or be required to provide sufficient guidance in securing PHI.

HHS Office for Civil Rights website (*http://www.hhs.gov/ocr/privacy/hipaa/understanding/*)

NIST 800 Series Special Publications (*http://csrc.nist.gov/publications/PubsSPs.html*)

In particular:

- NIST SP 800-36 Guide to Selecting Information Technology Security Products
- NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- NIST SP 800-88 Guidelines for Media Sanitization
- NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices
- NIST SP 800-114 User's Guide to Securing External Devices for Telework and Remote Access
- NIST SP 800-124 Guidelines on Cell Phone and PDA Security