

A Guide to Cybersecurity Basics for
Small Healthcare Practices

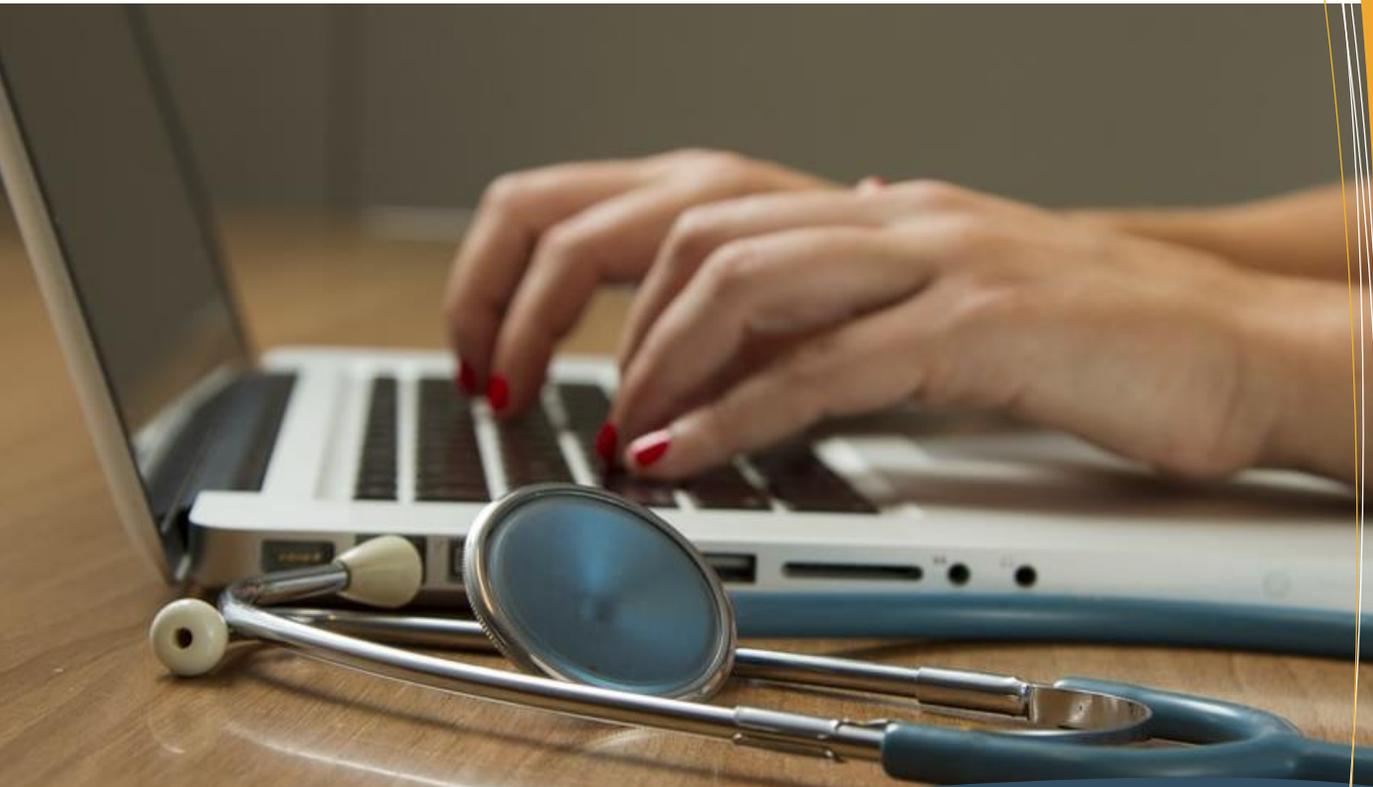


Photo by National Cancer Institute

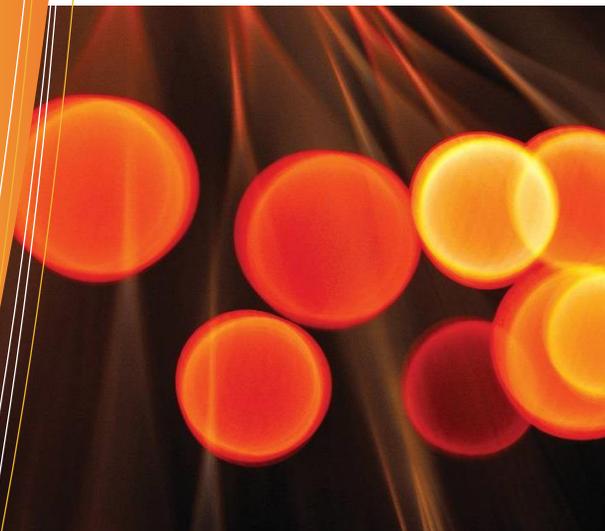
QUICK START GUIDE

For HIPAA Security Rule
Compliance



HOW A CYBERSECURITY INCIDENT CAN IMPACT A SMALL PRACTICE

- Loss of patient records
- Revenue lost during IT outages
- Replacement cost of IT assets
- HIPAA-related fines
- Reputation risk
- Stolen bank passwords or SSNs
- Interruption of patient care
- Inability to bill for services
- Risk of legal fees
- Detriment to staff morale



Protecting Patient Records Is Critical

Over the past two years, cybersecurity incidents and attacks in healthcare increased over 55% from the previous year and cost the industry thirteen billion dollars¹. With the COVID-19 pandemic dominating headlines and budget constraints threatening even the most basic of operations, healthcare organizations may be tempted to sacrifice cybersecurity, and to their own detriment. Small healthcare organizations face many of the same evolving cybersecurity risks as large organizations and a single cybersecurity incident can be financially catastrophic for a small practice.

Small healthcare practices don't have the luxury of a dedicated IT Shop

IT'S A MATTER OF EXPERTISE

Without the support of the Federal Government or the budget for a private consulting firm to bolster cybersecurity efforts, small healthcare practices are forced to adopt a DIY (Do It Yourself) approach to cybersecurity and privacy protection. With over 30 different cybersecurity specialty areas defined by the National Institute of Standards & Technology (NIST), this is no trivial task. Despite a lack of dedicated IT personnel and the necessary monitoring and response tools, small practices face the same level of risk and evolving threats as every other large company in the United States.

USING THIS GUIDE

This guide provides small practices with a basic understanding of the cybersecurity landscape, common risks facing the healthcare industry, and foundational activities needed to protect the digital systems and records your practice has come to rely on for daily business. This guide does not cover the full breadth and depth of HIPAA Security Rule, but serves instead as a first step.

¹ Source: *Muncaster, P. (2021, February 18)*



The HIPAA Security Rule

Most healthcare providers are familiar with the HIPAA Privacy rule and its requirements to protect patient confidentiality. Healthcare practices of any size are also subject to the HIPAA Security Rule. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the security of electronic protected health information. In short, the HIPAA Security Rule means basic cybersecurity isn't optional. No cyber defense is perfect, but at a minimum, implementing good cybersecurity practices mitigates liability risk in the event of a cybersecurity incident, demonstrating a good faith effort on the part of the organization to protect organizational data and patient information.

1. Develop Good Policy

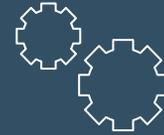
The foundation of any IT security program begins with information security policy. Fortunately, there is no need to reinvent the wheel when it comes to implementing information security policies. In the attachments, this getting started guide includes tailorable templates for the most common policy topics that can be adapted for use.

Information Technology policies should be provided to all staff, including temporary employees, during onboarding and annually thereafter. Employees should be required to sign or acknowledge the policies. Be sure to store policies in a centralized location, whether in hard copy or digital form, so they are always accessible to staff for reference.

As the cybersecurity program matures, the recommended approach to policy enhancement is the alignment of policy to the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)². As a step saver, the U.S. Department of Health and Human Services (HHS) provides a convenient [crosswalk](#) of the HIPAA Security Rule security requirements to the five CSF categories.

² Reference: [NIST Cyber Security Framework](#)

5 CYBER SECURITY BASICS Every Healthcare Practice Should Implement



1 CREATE RULES TO LIVE BY

Develop clear and concise policy that staff can understand and follow

2 CHOOSE PRODUCTS WISELY

Spend the time to research IT solutions that minimize cybersecurity burden



3 MAINTAIN GOOD CYBERSECURITY HYGIENE

Don't let information technology products collect dust, create a regular update schedule for vendor software

4 PRACTICE MAKES PERFECT

Put security practices in place to make security second nature, require frequent refresher training

5 HAVE A BACKUP PLAN

Assume a system outage is going to happen and have a backup plan that all staff can follow to maintain operations and recover data records, if lost or damaged



2. Choose Technology Wisely

While strong security policy and standardized practices form a critical foundation, policy alone is not enough. Good cybersecurity requires the intelligent selection, acquisition, configuration and maintenance of hardware and software. In healthcare, that means not only desktops, laptops, mobile devices, and communication systems but also medical devices and electronic health record solutions. While confidentiality is a key focus for privacy, the availability of IT and integrity of the data within is also an important consideration for healthcare practices. When acquiring any new technology, consider the following:

- **Define Business Need.** Focus clearly on the problem to be solved- more features and functionality may mean more security burden.
- **Consider Alternatives.** Compare the features, functions, and costs of at least 3 vendors. This [comparison table](#) may help.
- **Evaluate Security.** Know what security features come set as a default, versus those that must be added or customized later.
- **Securely Implement the Solution.** Make certain all customizable security settings have been properly configured and security maintenance responsibilities are well defined.



Shared Passwords Can Quickly Become a Common Practice Without Clear Policy Enforcement & Good Security Culture – Never Allow Shared Login Credentials

Strong cyber practices support good health for patients and providers

3. Maintain Cybersecurity Hygiene

Though they are trained to help their patients navigate complex and chronic conditions, healthcare professionals recognize the importance of basic hygiene practices like handwashing, good nutrition, and regular exercise as preventive measures for a multitude of ills. Just like these basic health practices, many cybersecurity issues can be avoided through consistent cybersecurity hygiene within your practice.

Just as good nutrition alone does not prevent cancer, implementing these practices cannot guarantee prevention of an attack. However, each step taken will reduce organizational risk and ensure progress toward protecting the data of both the practice and its patients. A few key hygiene items to start with:

- **Enforce Strong Passwords.** Use strong passwords, enforce changes regularly, and prohibit sharing of passwords. Consider moving to the use of verification codes at login, as this multi-factor technique is the single most effective way to combat theft of login credentials.
- **Update Software.** Every system component has some form of software that requires regular updates to keep secure. Vendors release updates to address newly identified security flaws with their software, a lot like recalls issued by automobile manufacturers. Much like the free repair for a known automobile recall issue, software vendors offer free patches to immediately close known vulnerabilities and prevent them from being exploited. Visit software vendor sites to register for email alerts and authorize automated version/patch updates wherever possible.



- **Install Anti-Virus/Anti-Malware Software.** Install antivirus software on every computer and system in the practice and set it to automatically update. Track the expiration of the license and set it to auto renew where possible to avoid unexpected gaps in coverage.
- **Create & Protect Data Record Backups.** Keep files secure by backing up important data offline, on an external hard drive, or in the cloud. This can help protect against many types of data loss, especially if bad actors gain access to one or more practice devices. Examine the encryption features of backup media. Always encrypt sensitive data to prevent any unauthorized access to patients' confidential data if equipment is lost, stolen, or compromised.

When it comes to hygiene, discipline leads to success. Assign responsibilities and mark the calendar with target completion dates for each series of tasks — things such as scanning for viruses with antivirus software, updating the operating systems of all devices, checking for security patches and changing passwords. Once staff begin to get the hang of cyber hygiene, it will become second nature.

4. Regularly Train Staff

The Healthcare Industry faces two primary threats that can be overcome through regular training: complacency among staff when it comes to privacy and security protocols; and social engineering attacks from bad actors who recognize the value of healthcare data.

When it comes to protocols for data privacy and security, *practice makes perfect*. At least once per year, all staff should be required to demonstrate their proficiency and compliance with cybersecurity practices related to their job duties.

Social engineering attacks entail an outside person or organization that manipulates a user with the intent to gain unauthorized access to systems or data. A social engineering attack can result in a breach through the simple action of clicking on a malicious link on the internet, opening an unsafe email attachment, or revealing login credentials to a hacker posing as IT support. Social engineering attacks exploit a common human desire to be helpful or a user's tendency to be curious.

Healthcare organizations are particularly vulnerable to attacks that disable, encrypt, or otherwise render useless their most valuable organizational data — patient records, in exchange for a large sum of money (records held for ransom). Ransomware attacks are frequently launched through malware embedded in a malicious link. This means falling prey to a ransomware attack is more likely if an organization is not maintaining proper cyber hygiene, including frequent staff training.

In October 2020, the FBI and the Cybersecurity and Infrastructure Agency released a special advisory alert noting “credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.” This alert was driven by a notable surge in ransomware attacks. Ransomware attacks now account for about half of all data breaches in healthcare.⁴

Ongoing awareness training can reduce the likelihood of a social engineering attack by up to 70%.

⁴ Source: *Muncaster, P. (2021, February 18).*

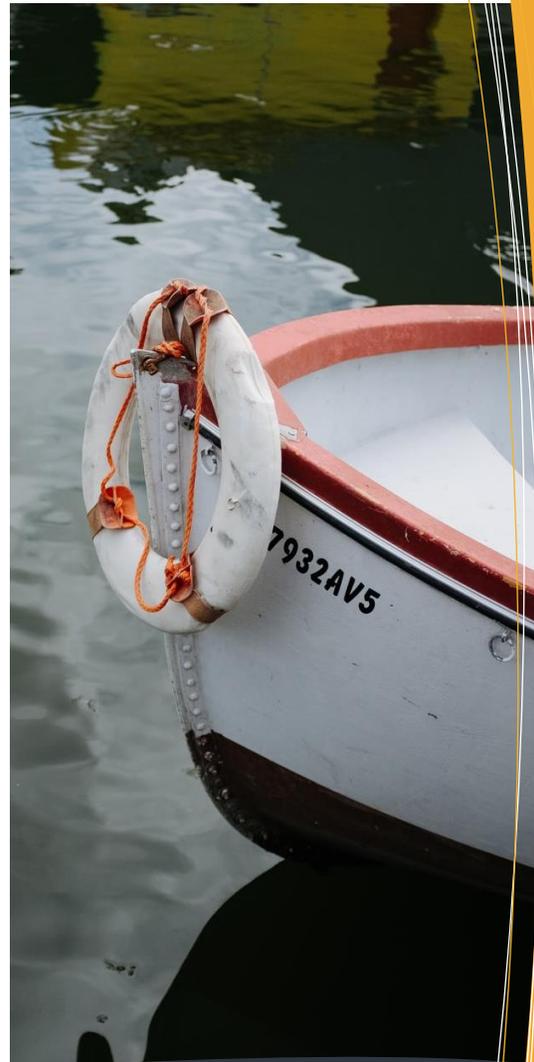
Healthcare organizations may find efficiency in tracking cyber security training alongside continuing education requirements. Ample free and low-cost training is now available from trusted government and nonprofit institutions. A sample training plan with links to some of these external training resources is provided in Attachment B.

5. Have A Backup Plan

Healthcare professionals who have completed their education in recent years are digital natives and will be naturally at ease with a variety of electronic medical records and digital devices. The tradeoff for this level of familiarity with technology is a lack of experience in working without it.

In the event of an outage, the practice must have a clear set of alternative work procedures instructing staff on how to proceed without the usual hardware/software tools. Any team can handle an outage of a few hours; but in the current cyber threat landscape, outages are lasting an average of 16 days³.

Things to consider and plan for include collecting payment, accessing patient records, and synchronization of data records post-incident. Employees should be required to review the plan annually and organizations should conduct an annual Table-Top Exercise to test the procedure to ensure employees are capable and confident in conducting business during an IT system outage. A sample test plan is included in Attachment C.



CALL TO ACTION

The HIPAA Security Rule applies to practices of all shapes and sizes. We've covered the basics. Whether you are following the DIY approach, or enlisting help from a company like CyberEye, you can establish or improve your cybersecurity program – STARTING TODAY.

- Establish HIPAA Policy
- Identify IT Products & Apply Security Settings
- Create an IT Backup Plan
- Train Staff on Policy & Plans
- Assign Cyber Hygiene Processes
- Review Program Annually

³Source: Palmer, D. (2020, January 23).

A PUBLIC/PRIVATE PARTNERSHIP: HARNESSING THE POWER OF ACADEMIA & INDUSTRY

CyberEye, a commercial services provider in the field of information security governance, risk and compliance, is pleased to present this free Quick Start Guide as a resource for healthcare practices.

The Quick Start Guide was prepared as a collaborative academic project between CyberEye and the University of South Carolina, through the Master's of Health Information Technology Program. The University of South Carolina prepares students with expertise in management of both health care systems and information technology. Blending technology curriculum with course work covering current clinical trends, government regulations and healthcare-specific practices, this Program is designed to create a highly skilled workforce and lead the industry in technologically advanced and efficient health care systems.

This engagement reflects the interest and commitment of both USC and CyberEye to foster ongoing collaboration between academia and industry, providing significant benefits to healthcare providers, and patients.

ABOUT THE AUTHOR



Maria Petrie, CISSP, HCISPP is a Registered Nurse and seasoned cybersecurity consultant who brings a passion for clinical transformation powered by technology. Prior to specializing in healthcare, Maria spent more than a decade advising Federal Government clients on matters of cybersecurity policy and governance.

Leveraging her past experience coaching a new healthcare practice through an avoidable HIPAA security & privacy incident, Maria brought lessons learned to this Quick Start Guide as part of her Master's of Health Information Technology Program at the University of South Carolina. She sought out collaboration with CyberEye to transform the academic exercise into practical application, bringing the Guide to life as a resource for small healthcare practices.

ABOUT CYBEREYE



After over 20 years of specialized experience building transformational cybersecurity programs for Federal Government and Commercial clients, Kim Maurer established CyberEye, to bring affordable, and realistic roadmaps for governance, risk and compliance to small and mid-sized companies.

CyberEye was founded on the belief that building, implementing and maintaining cyber programs can and should flex with the changes of a growing business. CyberEye offers customizable consulting services for HIPAA compliance and program implementation. Visit cybereyesolutions.com to learn more.