TOP TEN Cyber Security Tips for Small Health Care Organizations

All health care organizations need a cybersecurity strategy to support business continuity, maintain the confidentiality of administrative, clinical, and financial information and preserve patient safety. The threat from cyberattacks is growing exponentially and smaller health care organizations are particularly vulnerable.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires all health plans, providers, and clearinghouses (i.e., covered entities) to implement and maintain appropriate policies and procedures to ensure health information is kept secure while being used, transmitted, or stored. Small health care organizations are encouraged to implement and regularly review and update security measures to stay protected. Below are suggested actions that small organizations can adopt, customize, and implement as they seek to establish good cyber hygiene.*

1 **IDENTIFY A CYBERSECURITY CHAMPION.** Establish this formal role to lead and promote cybersecurity hygiene across the organization. This role's scope should include information technology, compliance, business operations, and should be understood and prioritized. The Cybersecurity Champion will lead ongoing security education, workforce member awareness (and ongoing activities such as Cybersecurity days/weeks/fire drills) and facilitate the organization's response to a cyber event. The Cybsersecurity Champion's job description should reflect these overall responsibilites as well as include ongoing professional opportunities to ensure the organization stays current with evolving changes.

2 **TRAIN WORKFORCE IN SECURITY PRINCIPLES.** Establish basic security practices and policies for all full-time and part-time members of your workforce (e.g., require strong passwords, and establish appropriate Internet use guidelines). Establish rules of behavior describing how to handle and protect customer information and other vital data. Train workforce on basic Internet use best practices to prevent cyberattacks. Training topics to cover include:

- Spot phishing emails.
- Require sound Internet browsing practices, including when not to open emaills, attachments, or links from unfamiliar senders. Report suspicious messages to internal IT team or the designated point-of-contact for external IT vendor.
- Enable authentication tools (e.g., strong passwords, Multi-Factor Authentication, etc.)
- Protect sensitive vendor and customer information.
- Maintain physical security (including mobile devices).
- Leverage document shredding processes and tools.
- Erase data and destroy hard drives appropriately.
- Develop and deploy response and contingency plans.

3 **PROTECT INFORMATION, COMPUTERS, AND NETWORKS FROM CYBERATTACKS.**

A. CONDUCT AND MAINTAIN A SECURITY RISK ASSESSMENT (SRA).

- The HIPAA Security Rule requires that covered entities and business associates conduct an SRA of their organization to guide implementation of relevant HIPAA administrative, physical, and technical safeguards.
- As part of the SRA, create an inventory of the organization's information assets, including data, ePHI, and systems that touch the ePHI. All ePHI that is created, received, maintained and transmitted by the organization should be documented as part of a comprehensive SRA. The systems that support ePHI transactions should be identified and maintained in an Asset Inventory (a spreadsheet or an automated tool) to enable an accurate and current SRA.

B. KEEP CLEAN MACHINES.

- Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. The organization's computers should be equipped with latest antivirus software and are updated regularly. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.
- Configure all software to install updates automatically. Update software associated with operating systems, web browsers, and other applications.If outsourcing IT support, ensure the service provider's contract upholds network and software security.

C. SECURE ENDPOINTS.

- An endpoint is any device that workforce members and contractors use to connect to the organization's network, including desktops, laptops, mobile phones, and tablets. These devices represent possible gateways that could be exploited to steal data and hijack networks and must be protected.
- Even software applications and integrated platforms or APPs that get installed can be considered endpoints. Endpoint security solutions protect the entire organization's network rather than just individual devices.

D. MAKE BACKUP COPIES OF IMPORTANT ADMINISTRATIVE AND CLINICAL DATA AND INFORMATION.

- Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, accounts receivable/payable files, clinical records, and other information.
- Backup data automatically if possible, or at least weekly, and store the copies either offsite or in the cloud. If using an IT cloud platform, ensure that the cloud service provider contracts contain data storage/backup commitment and verify compliance.
- Be sure to test the availability of the data in the backup on a routine basis.

E. LIMIT WORKFORCE ACCESS TO DATA AND INFORMATION, LIMIT AUTHORITY TO INSTALL SOFTWARE.

- Do not provide any one staff member with access to all data systems. They should only be given access to the specific data systems that they need for their jobs (minimum necessary) and should not be able to install any software without permission.
- Once an individual leaves the organization, their system user profile should be de-activated or terminated in a timely manner. Physical access to the premises should be revoked immediately, and all keys/passcodes retrieved. Remote access to computers from these former staff should also be terminated immediately.

F. CONTROL PHYSICAL ACCESS TO YOUR COMPUTERS AND CREATE USER ACCOUNTS FOR EACH WORKFORCE MEMBER.

Prevent access or use of organization computers by unauthorized individuals. A separate user account must be created for each individual and require the use of strong passwords (at least 12 alphanumeric with special characters). Administrative privileges should only be given to designated IT staff and key personnel. Conduct access audits on a regular basis to ensure that former workforce members have been removed from your systems and have returned all company issued devices.

Use technical configuration best practices, such as setting the computers to automatically log out after a determined inactive period of time.

G. CREATE A MOBILE DEVICE ACTION PLAN.

Laptops, tablets, and smart phones that contain administrative and/or clinical data can be easy targets for theft or can be lost. Require users to password-protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Set reporting procedures for lost or stolen equipment.

TOP TEN Cyber Security Tips for Small Health Care Organizations

4 PROVIDE FIREWALL SECURITY FOR YOUR INTERNET CONNECTION AND MONITOR YOUR NETWORK. A firewall is a set of related programs that prevent unauthorized individuals from accessing data on a private network. The operating system's firewall should be enabled. Set firewall configurations to "deny all – allow by exception only" as a best practice. For remote workers, home system(s) should be protected by a firewall. Implement automated monitoring tools (i.e., Intrusion detection systems and intrusion prevention systems, IDS/IPS) on the network to identify potential incidents, log information, alert appropriate personnel, and stop the potential incident from becoming a true event.

5 SECURE YOUR DATA AND NETWORKS. Encryption is the process of changing plain text to "cyphertext" using mathematical codes (i.e., encryption keys) to conceal the original data, and requires a decryption key to convert cyphertext back to plain text for usage. Encrypt your data while in transit (processing) or at rest (stored) to protect it from being stolen, modified, or compromised. Safeguard Internet connections by encrypting information and using a firewall. If your organization has a Wi-Fi network, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password-protect access to the router. If you have remote workers, use a Virtual Private Network (VPN) to allow secure connection to the network. Create a separate Guest Wi-Fi network to allow visitors, patients, and customers public internet access.

6 EMPLOY BEST PRACTICES ON PAYMENT CARDS. Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. Additional security obligations that are pursuant to agreements with banks or processors may exist. Isolate payment systems from other, less secure programs. Do not use the same computer to process payments and browse the Internet.

7 USE STRONG PASSWORDS AND MULTI-FACTOR AUTHENTICATION.

- Require workforce members to use unique and strong passwords and change passwords a minimum of every three months. Do not allow passwords to be written down, and encourage the use of automated password managers.
- MFA is a mechanism to verify an individual's identity by requiring them to provide more than just a typical username and password. MFA commonly requires users to provide two or more of the following: something the user knows (password, phrase, PIN), something the user has (physical token, phone), and/or something that physically represents the user (fingerprint, facial recognition). All access to network and applications with sensitive/ confidential/protected data must be through MFA.

8 MONITOR AND MANAGE CLOUD SERVICE PROVIDER (CSP) ACCOUNTS. Consider using a CSP to host your organization's information, applications, and collaboration services, especially if you're utilizing a hybrid work structure. Software-as-a-Service (SaaS) providers for email and workplace productivity can help secure data. Be sure to clearly understand the scope of the organization's responsibilities as compared to the CSP's in this contractual service relationship. The CSP Shared Responsibility Matrix should be a part of the contract discussion and negotiate the shared accountability model.

9 CONTRACT FOR OUTSIDE IT SUPPORT. Smaller health care organizations may not have the in-house expertise to upgrade and monitor IT systems and help develop appropriate cybersecurity defenses. Consider identifying an outside consultant or IT support company to assist in the purchase and ongoing support of IT systems and development of cybersecurity policies and procedures. Conduct due diligence on outside IT (including any Cloud services) support, and obtain the required Business Associate Agreement, periodically check that the service level agreement (SLA) metrics are being met. Although an outside entity is responsible for your day-to-day IT operations and cybersecurity controls, you are still primarily accountable for Security compliance.

10 DEVELOP REACTION, CONTINGENCY, AND RECOVERY PLANS. Develop an action plan specific to your organization to (i) react quickly to a cyberattack on your organization or one of your operational partners; (ii) identify contingencies to prepare for administrative and clinical operational continuity; and (iii) recover from a cyberattack. Action steps include:

- Develop an internal process to identify a cyber issue as quickly as possible and identify an individual responsible for coordinating the response.
- Work with your IT department or outsourced IT firm to identify what the issue is, how it is likely to impact your organization, and impact severity.
- Determine the immediate steps to maintain patient safety.
- Ascertain the individuals and business partners to be contacted (these could include patients to be rescheduled, referring offices to be notified, and members/clients to be informed).
- Identify local, state, and federal officials that must be informed of the situation and contact them. (Note: In case of a data breach involving more than 500 individuals, the federal government, local media, and the impacted individuals themselves must be notified without delay.)
- Create contingencies, aka workaround processes, which could include dropping to paper records and paper billing. Test these contingencies internally and with your business partners.
- Establish a line of credit at a local financial institution should a business partner's cyberattack impact your revenue stream.

* This document was developed by the Workgroup for Electronic Data Interchange (WEDI). WEDI is a nonprofit, multi-stakehollder organization named in HIPAA as an advisor to the Dept. of Health and Human Services. All content is for educational purposes only. WEDI does not intend for the content to be a substitute for professional, legal or consultative advice.

SCAN THIS QR CODE OR GO TO WWW.WEDI.ORG FOR A LIST OF FREE SECURITY RESOURCES FROM THE FEDERAL GOVERNMENT.