afmc℠ HIPAA WATCH

JUNE 2019

Top 10 Tips for Cybersecurity in Health Care

Cybersecurity protections are keenly important for health care data and information systems to protect patient health-information from attack and disruption. Cybersecurity refers to ways to prevent, detect and respond to attacks or unauthorized access against a computer system and its information.

These 10 tips were developed to help small health care practices apply cybersecurity and risk management principles; however, their careful use can benefit any type of organization. Adoption of these tips is not a guarantee of compliance with federal or state law, but it can help organizations work toward the goal of having in place appropriate cybersecurity protections.

1. ESTABLISH A SECURITY CULTURE

- **Build a security-minded organizational culture** so that good habits and practices are automatic.
- **Conduct information security education and training frequently**, on an ongoing basis.
- **As a manager and leader, set a good example** in attitude and action toward security.
- **Instill "take responsibility for information security"** as one of your organization's core values.

2. PROTECT MOBILE DEVICES

- **Ensure mobile devices are equipped** with strong authentication and access controls.
- **Ensure laptops have password protection** (see examples in Tip 8).
- **Enable password protection on hand-held devices (if available).** Take extra physical-control precautions over the device if password protection is not provided.
- **Protect wireless transmissions from intrusion** (see Tip 9).
- **Do not transmit unencrypted protected health information (PHI)** across public networks (e.g., Internet, Wi-Fi).
- **Encrypt PHI data that is absolutely necessary** to commit to a mobile device or when removing a mobile device from a secure area.
- **Do not use mobile devices that cannot support encryption.**
- **Develop and enforce policies specifying the circumstances** under which devices may be removed from the facility.
- **Take extra care to prevent unauthorized viewing** of the PHI displayed on a mobile device.

3. MAINTAIN GOOD COMPUTER HABITS

- **Uninstall any software application that is not essential to running the practice** (e.g. games, instant message, photo sharing tools) or no longer needed.
- **Keep software up-to-date when new versions become available** because updates can include security features and PHI protections.
- **Disable user accounts of former employees in a timely manner.**
- **"Sanitize" before disposing all data stored on computers and other devices,** including copy machines.

4. USE A FIREWALL

- **You must install a firewall to protect against intrusions and threats from outside sources,** unless your electronic health record (EHR) system is totally disconnected from the internet.
  - 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 developers.
- **Consider a hardware firewall if you are a large practice** that uses a local area network (LAN).
  - A hardware firewall sits between the LAN and the internet, providing centralized management of firewall settings.
  - Hardware firewalls should be configured, monitored and maintained by a specialist.

5. INSTALL AND MAINTAIN ANTI-VIRUS SOFTWARE

- **Use an anti-virus product that provides continuously updated protection** against viruses, malware and other code that can attack your computers through web downloads, CDs, email and flash drives.
- **Keep anti-virus software up-to-date.** Most software automatically generates reminders about updates; many can be configured to allow for automated updating.

6. PLAN FOR THE UNEXPECTED

- **Create data backups regularly and reliably.**
  - Begin backing up data from day one of a new system.
  - Ensure the data is being captured correctly.
  - Ensure the data can be quickly and accurately restored.
  - Use an automated backup system, if possible.
- **Consider storing the backup far away** from the main system.
- **Protect backup media** with the same type of access controls described in Tips 7 and 10.
- **Test backup media regularly** for the ability to restore data properly, especially as the backups age.
- **Have a sound recovery plan that tells you:**
  - What data was backed up (e.g., databases, pdfs, tiffs, docs)
  - When the backups were done (timeframe and frequency)
  - Where the backups are stored
  - What types of equipment are needed to restore them
- **Keep the recovery plan at a secure, remote location** where someone has responsibility for producing it in an emergency.

7. CONTROL ACCESS TO PHI

- **Configure your EHR system to grant PHI access on a need-to-know basis.**
  - This access control system might be part of an operating system (e.g., Windows), or built into an application (e.g., an e-prescribing module) or both.
- **Manually set file access permissions using an access control list.**
  - This can only be done by someone with authorized rights to the system.
  - Prior to setting these permissions, identify what files should be accessible to which staff members.
- **Configure role-based access control as needed.**
  - In role-based access, a staff member's role within the practice (e.g., physician, nurse, billing specialist) determines what information may be accessed.
  - Assign staff access to the correct roles and set access permissions for each role correctly, on a need-to-know basis.

8. USE STRONG PASSWORDS AND CHANGE THEM REGULARLY

- **Select passwords that are not easy to guess. Strong passwords include:**
  - At least eight characters long; the longer the better
  - A combination of uppercase and lowercase letters, at least one number and one special character, such as a punctuation mark
  - Should not include personal information such as:
    - — Birth date
    - — Names of self, family members or pets
    - — Social Security number
    - — Anything on your social networking sites or that could easily be discovered
- **Require multifactor authentication.** If you e-prescribe controlled substances, you must use multifactor authentication for your accounts. It combines multiple authentication methods, such as a password plus a fingerprint scan, resulting in stronger security protections.
- **Update passwords regularly.** Configure your systems so passwords must be changed.
- **To discourage staff from writing down passwords, develop a password reset process that provides quick assistance for forgotten passwords.** This process could involve authorizing two staff members to reset passwords, or select a product that has built-in password reset capabilities

9. LIMIT NETWORK ACCESS

- **Prohibit staff from installing software** without prior approval.
- **When a wireless router is used,** set it up to operate only in encrypted mode.
- **Prohibit casual network access by visitors.**
- **Be sure filesharing, instant messaging and other peer-to-peer applications** have not been installed without explicit review and approval.

10. CONTROL PHYSICAL ACCESS

- **Track all devices and monitor their locations.** If a device is lost, take steps to lock down and recover the device.
- **Store devices behind locked doors** or in secure areas.
- **Monitor employee access to the property,** limit keys/keycodes and manage access when staff leave the organization.

FOR MORE INFORMATION:

Additional details and sample checklists for each area can be found at:
https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

For more information about this issue of **AFMC *HIPAAwatch***,
or AFMC's Security Risk Analysis (SRA) services,
contact AFMC at **SRA@afmc.org** or 501-906-7511.