JMARK
BUSINESS SOLUTIONS, INC.
Your Complete IT Services Partner

STAY OFF THE WALL OF SHAME

ESSENTIAL I.T. SECURITY TIPS FOR YOUR MEDICAL PRACTICE AND BUSINESS ASSOCIATES

WWW.JMARK.COM

The following are some essential I.T. security tips for your medical practice and business associates.

Due to the explosive growth of Electronic Medical Records (EMRs) and electronic Personal Health Information (ePHI), medical practices and their associates are at risk from cyber attacks and possible HIPAA non-compliance. With so much digital patient data being created each day, medical sites are prime targets for criminals who wish to steal the data and sell it on the dark web.

Although the regulations for HIPAA and EMR security have become more stringent, there's no particular technology blueprint from the Office of Civil Rights that you can implement to stay compliant — they do not prescribe a specific firewall, model number, or solution.

Implementing security best practices is vital. Here are a few common risks that threaten your business.

What can you do to stay off the wall of shame?

Improve your data security.

EMR Theft: Protecting your physical environment is vital. Criminals break into medical offices to steal patient files and take computer equipment. They even break into cars to grab laptops containing confidential information.

Employee Malice: Disgruntled employees intentionally delete data and share it on the internet. The reasons are varied. Some do it for monetary gain, some for revenge.

Employee Accidents: Human error is a common security risk. Employees get so busy and distracted that they accidentally delete patient data. Without a proper backup solution, files that have been deleted are lost forever. Another example is employees surfing the internet and inadvertently downloading ransomware which encrypts files and renders them useless.

Ransomware: As noted above, criminals encrypt data for a ransom payment. They often cover their tracks by demanding payment in Bitcoin, an anonymous form of money transfer. If you do not pay, the patient data remains encrypted and is essentially lost.

Hacking: Criminals are always looking for a way to break into networks. Under HIPAA, breach notifications are mandatory. An organization which has suffered such an incident has their practice displayed on the HHS Wall of Shame. There were 28 additions to the list in July 2018, with more undoubtedly added in ensuing months.

Here Are 7 Best Practices

(Work on them bit by bit over the next week to improve your data security.)

1. Email:

- ***Know where your email is hosted.*** Some practices are still using Gmail, AOL, Yahoo, or GoDaddy. These email platforms do not comply with HIPAA, as that would require them to sign a Business Associate Agreement (BAA), which is highly unlikely.

- ***Host your email on Office 365 or Google Apps.*** If you choose Google, then ensure you use your own domain (as in yourname@yourmedicalpractice.com). Internal email servers are also acceptable. However, it's far more cost effective to have someone else host your email for you.

- ***You must protect ePHI from being emailed.*** It's essential that you have policies in place to prevent the sending of ePHI via email. In addition, you also need to encrypt confidential data. Here's what to do:

> **Sign up for Office 365 or Google Suite. (Microsoft or Google can help you.)**
> - Set up an email address with your domain (not simply "@gmail.com").
> - Use an address like drsmith@yourmedicalpractice.com
>
> **Sign up for encryption.**
> - Get a BAA from your encryption company.
> - Get the encryption from Sophos or GoDaddy.
>
> **Create (and enforce) a policy prohibiting the emailing of ePHI unless it is encrypted.**

2. Data Storage:

- ***Your hosted EHR is responsible for storing and encrypting your data.*** You must have a policy in place which ensures this. Personal accounts on Drobox, Google Drive, or another personal cloud service are not permitted. You must enroll a business account that has the necessary management features.
- ***If your EHR is stored in-house, you need to make sure it's on a server that's protected. Virtually and physically.*** Ensure your server is in a locked room and that only authorized individuals can access it. Do not store your EHR on random workstations or mobile devices. If your doctors keep ePHI on their laptops and they're stolen, you are in breach of HIPAA.
- ***Review all workstations for out-of-band ePHI.*** If your receptionist has patient data on her desktop (out-of-band ePHI) and someone can view it, it's vulnerable unless it's secured and backed up.
- ***Create a policy stating no data can be stored on personal cloud solutions.***
- ***Create a policy for handling drives with ePHI, including disposal.*** This is one of the issues you'll see on the Wall of Shame. A stolen hard drive or laptop is a data breach.
- ***Sign up for HIPAA-compliant cloud storage.*** Office 365, Dropbox for Business versions only.
- ***Always get a BAA from your cloud provider.***

3. Data Backup:

An unsecured backup drive is a security risk. Audit your environment and make sure it's being backed up, including all your drives, laptops, and workstations. Ask your I.T. professional to ensure you have a resilient backup strategy.

- ***Your data needs to be secured onsite.*** In addition, a copy must be stored offsite in the event your office is destroyed by fire or flood.
- ***The offsite location must be HIPAA compliant.***
- ***Backups must be tested.***
- ***A full image of your server is optimal.*** Just backing up the files isn't enough when you need to recovery rapidly.
- ***Remember that all hardware fails at some point.***
- ***Ransomware is exploding.*** The only way to recover from ransomware is with backups. Employee cybersecurity training can help mitigate this threat.

4. Encryption:

The HHS Wall of Shame is filled with lost and stolen data. Thousands of laptops are left at airports in TSA. Hardware often mysteriously "walks away" from medical offices. And yes, this includes something as utilitarian as an external hard drive. For this very reason it is essential to encrypt data on your servers, laptops, workstations, and hard drives.

- ***Microsoft Windows provides encryption.*** Bitlocker is Microsoft's encryption tool, but it is only available with the Windows Professional package.
- ***Apple OSX has FileVault that you can use for encryption.*** Both Microsoft and Apple support encryption on external drives as well.

5. Physical Security:

A server must be locked away in a secure room. Under the desk in the lobby is not an acceptable location. Your backup server must also be secured in the same way, and both must be encrypted.

- ***Move your server to a locking closet.***
- ***If a closet isn't available, chain it to a wall in a locked cabinet in a private area, not the lobby!***
- ***Lock your laptops to carts or desks.***
- ***Secure your office space with an alarm system.***
- ***Whenever employees leave, make sure you change your locks and relevant passwords.***

6. Network Access:

You must know who has access to your data at all times, even when you're not there. Are your computers locked when employees leave their workstations? Can any unauthorized party access and use your computers?

- ***Periodically review your user accounts:***

  - Audit accounts and changes.
  - Remove old employees.
  - Correct levels of access.
  - Does everyone need access to all documents?
  - Limit access through permissions with the minimum access necessary.
  - Have unique accounts for each employee by name ("Ralph Smith" rather than "Receptionist").

- ***Review your wireless networks.***

  - Is your guest wireless on the same network as your medical records?
  - Log on and check. Can you access your data from your guest network?

- ***Do you have an appropriate firewall?***

  - Does your firewall actually prevent network attacks?
  - Does it perform updates automatically?
  - Fortinet/Cisco or Meraki are good enterprise grade options if you are looking for a firewall.

7. Training:

Training is critical because most data breaches are caused by human error. Even smart users need reminders and refresher training. Criminals are getting smarter and sending realistic-looking emails, writing something that tempts users to click malicious links. This technique, known as phishing, can help criminals steal login credentials or infect your network with malware.

- ***Your employees need to know what a safe link looks like and when not to open attachments.*** Identifying malicious emails, how to create secure passwords, and how to encrypt data are just some of the topics which should be covered by their training.
- ***Call your I.T. provider; they can help you with this training.***

Following these steps is a good start, but there is much more information you need to know to protect your practice. Work with a reliable, experienced I.T. service provider to increase your cybersecurity and ensure that your facility is compliant. Stay off the Wall of Shame for good!