Stay Off the **Wall of Shame**

Essential IT Security Tips for Your Medical Practice and Business Associates

The following are some essential IT Security Tips for Your Medical Practice and Business Associates.

Because of the explosive growth of EMRs and ePHI, medical practices and their associates are at security risk for cyberattacks and possible HIPAA non-compliance. With all the digital patient data floating around these days, it's prime time for criminals to pilfer it and sell it on the dark web.

Although the regulations for HIPAA and EMR security have become more stringent, there's no specific blueprint from the Office of Civil Rights to help you stay compliant — There's no firewall, model number or particular solution that they provide.

You must implement Best Technology Practices. What's occurred in other practices that you need to watch out for?

What can you do to stay off the Wall of Shame?

Improve Your Data Security.

EMR Theft: Criminals break into medical offices and steal patient files. Or they'll walk by a desk and take a computer. They even break into cars to grab laptops containing confidential information.

Employee Malice: Disgruntled employees intentionally delete data and share it on the Internet. They do this because they're angry with the boss or others in the office.

Employee Accidents: This is very common. Employees get so busy and distracted that they accidentally delete patient data. Without a proper backup solution, these files are lost forever. Or, when surfing the Internet, employees have accidentally clicked on a file with a virus that encrypted patient files so they can no longer be used. (This is called ransomware.)

Ransomware is everywhere: As noted above, criminals encrypt data for a ransom payment. They demand that is comes via Bitcoin, an anonymous form of money transfer. If not paid, they erase patient data.

Hacking: This is where criminals focus on one practice to steal their data. Once breached, HHS posts the names of these practices on the HHS WALL OF SHAME. There were 28 additions to the list in July 2017, and more added in August and September.

Here are 7 Best Practices to work on.

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

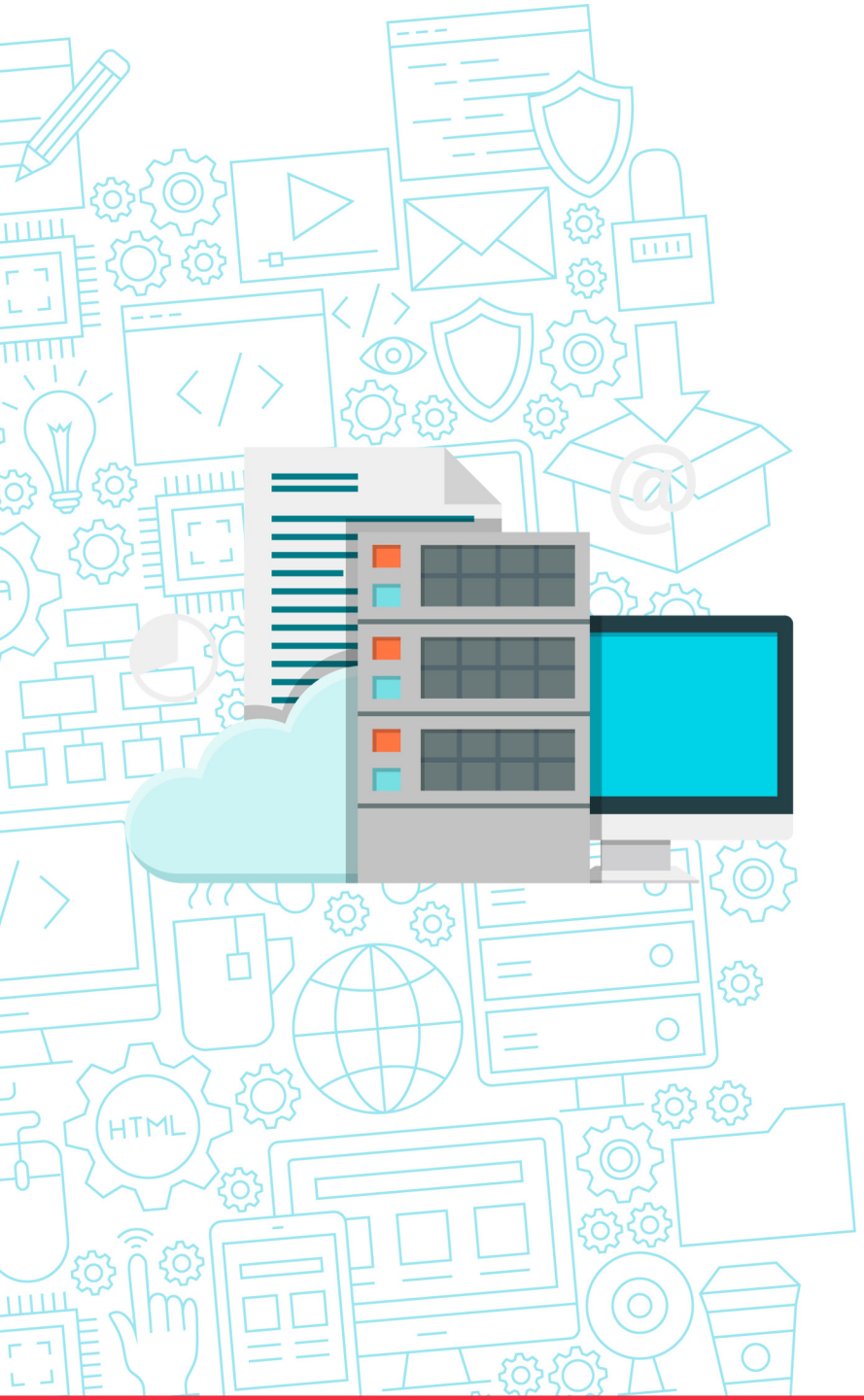
1. Email:

• **You must know where your email is hosted.** (Some practices are still using Gmail, AOL, Yahoo or GoDaddy). These email systems aren't compliant; you'll never be able to get a Business Associate Agreement (BAA) from them (which is necessary to be compliant with HIPAA).

• **Your email should be on an Office 365 solution, or Google Apps** (and not at gmail.com — Instead it should be yourname@yourmedicalpractice.com). You can also set up your own internal email server, or internal exchange server. These are acceptable. (However, it's cheaper to pay Microsoft to host your email on Office 365 than to keep email in-house.)

• **You must also protect your ePHI from being emailed.** It's essential that you have Policies in place to do this—As well as an Encryption Service to protect your confidential data. Here's what to do:

- Sign up for Office 365 or Google Suite. (Microsoft or Google can help you.)
  - o Set up an email address with your domain (not@gmail.com)
  - o Use an address like drsmith@yourmedicalpractice.com
- Sign up for encryption for at least your key people.
  - o Get a BAA from your encryption company.
  - o Get the encryption from Sophos, GoDaddy.
- Create a Policy for not emailing ePHI unless it's encrypted.



2. Data Storage:

• **Your hosted EHR is responsible for storing and encrypting your data.** You must have a policy in place to define this. Make sure you aren't hosting this data on Drobox, Google Drive or another personal Cloud service. You need a business account.

• **If your EHR is stored in-house, you need to make sure it's on a server that's locked that no unauthorized person can get to.** This is your responsibility. Do NOT store your EHR on random workstations, laptops, etc. If your doctors keep ePHI on their laptops and they're stolen, you're in trouble.

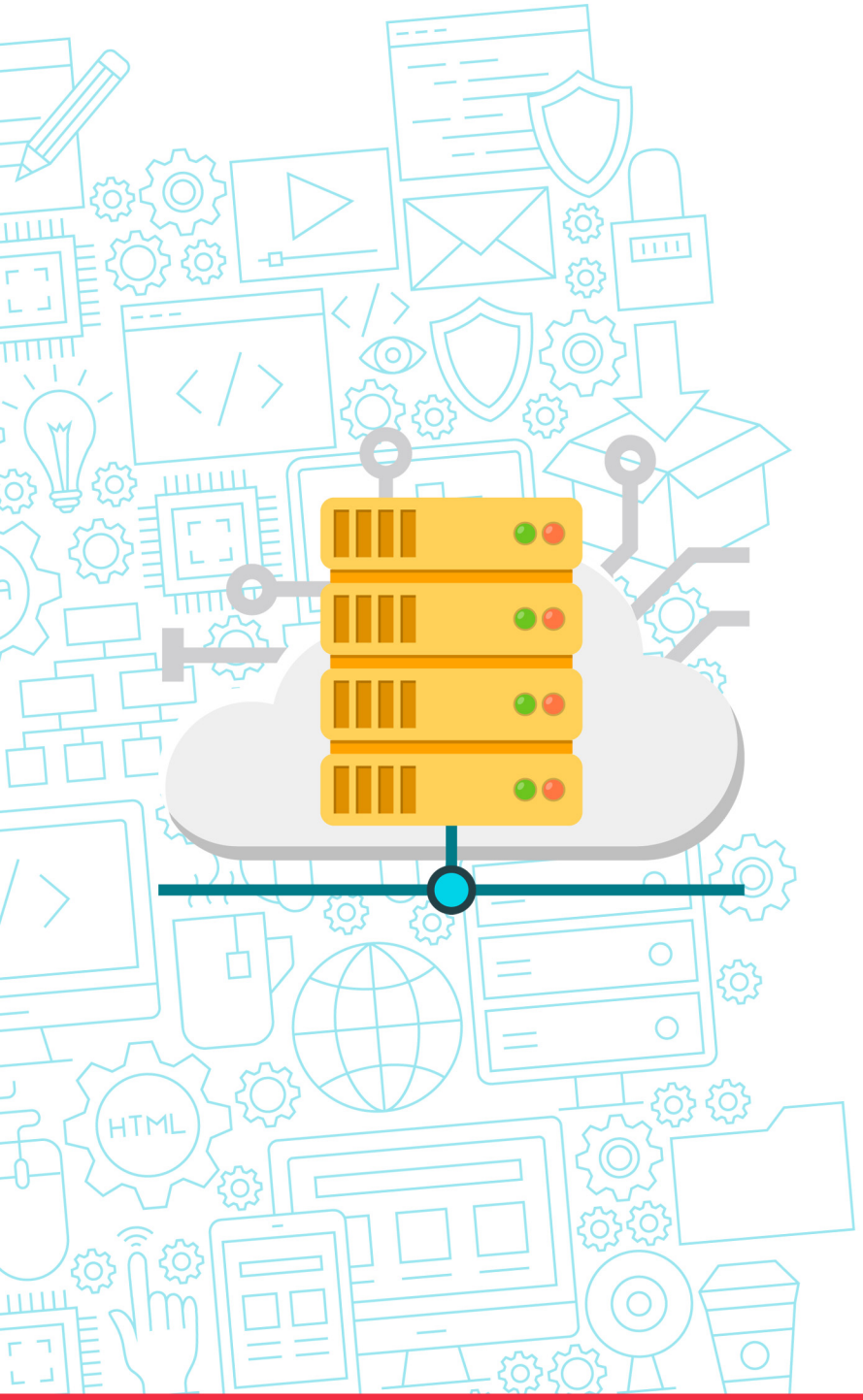
• **Review all workstations for out-of-band ePHI.** If your receptionist has patient data on her desktop (out-of-band ePHI) and someone stops by, it's vulnerable unless it's secured and backed up.

• **Create a policy for not storing data within 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. Someone breaks into your employee's car and steals your hard drive; or an old hard drive with ePHI is disposed of and the data is stolen.

• **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:

We see so many problems with backups when we go to medical practices. A backup drive will be sitting out in a reception area where anyone can grab it. Go through everything and make sure it's being backed up, all your drives, laptops, etc., too. If your server failed, how long would it take to get you back in business? Ask your IT professional.

- **Your data needs to be secured onsite,** and also stored offsite in case your office is destroyed due to fire or flood.
- **The offsite location must be compliant with HIPAA.**
- **Backups must be tested.**
- **A full image of your server is optimal.** Just backing up the files isn't enough.
- **Always protect against the unplanned.**
- **Remember that all hardware fails at some point.**
- **Ransomware is exploding.** (Employee cybersecurity training is essential.) The only way to recover from ransomware is with your backups.

4. Encryption:

The HHS Wall of shame is filled with lost and stolen data. Thousands of laptops are left at airports in TSA. Plus, they "walk away" from medical offices or are stolen — This includes external hard drives. This is why your servers, laptops, workstations, hard drives, and all data must be encrypted.

- **Microsoft Windows provides encryption,** but you must be using the professional version of Windows — It comes with BitLocker.
- **Apple OSX has FileVault that you can use for encryption.** Both Microsoft and Apple support encrypting on external drives as well.

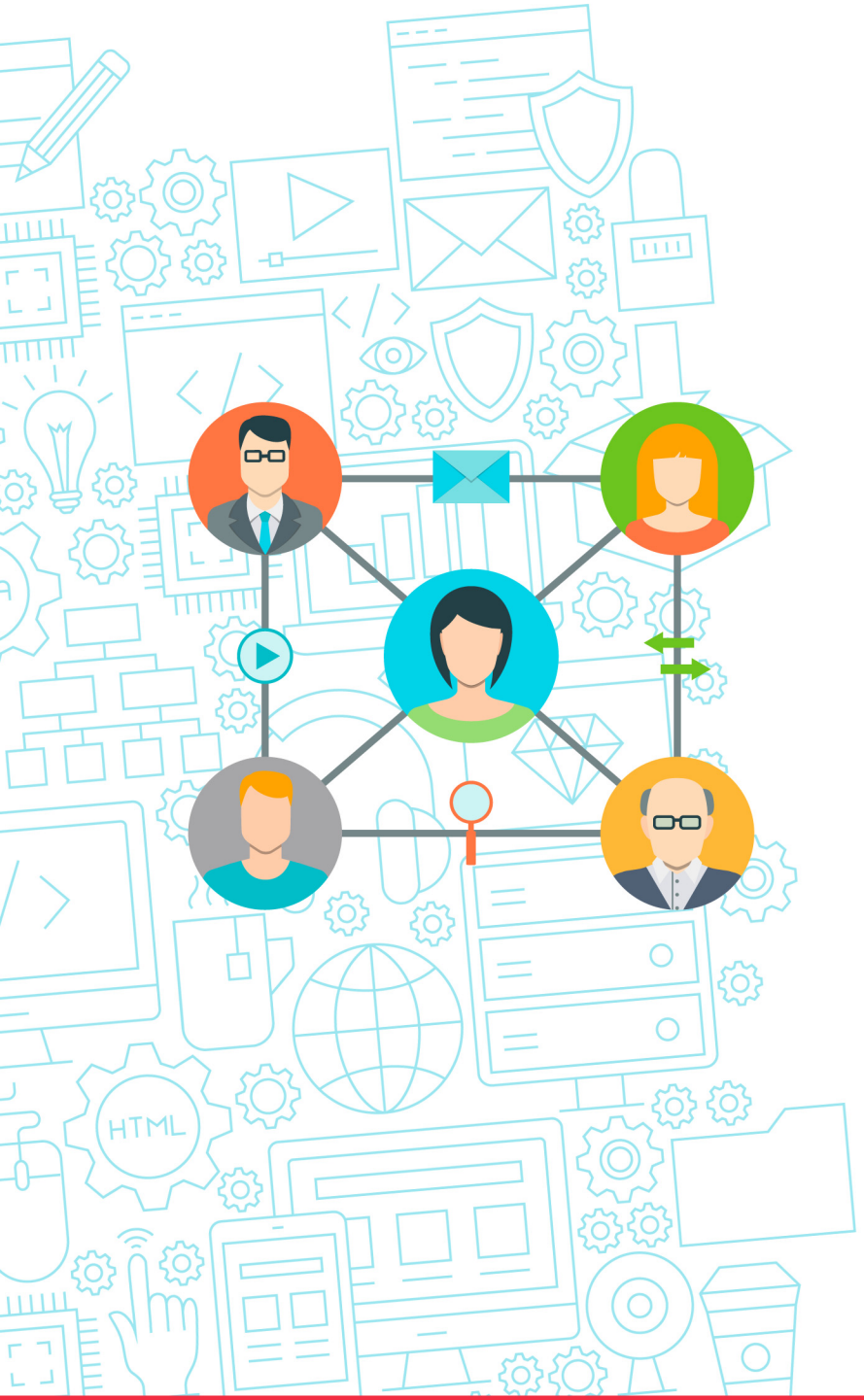
5. Physical Security:

This is a big issue with medical offices. Many try to use every bit of space for their patient needs and don't think about where the best place is for their server. Under the desk in the lobby isn't an acceptable location. Your backup server must be locked up where it's only accessible by your IT professional or other authorized person. (Plus remember to encrypt it.):

- **Move your server to a locking closet.**
- **If a closet isn't available, chaining it to a wall in a locked cabinet** may be acceptable (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 out your keys.**

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 walk away? Does your cleaning crew use your computers? (We've been in places where computers aren't locked and the cleaning crews have access. Sometimes a mom and pop cleaning crew brings their kids with them, and the kids play on the computers!)



- **Periodically review your user accounts:**
  - o Audit accounts and changes.
  - o Remove old employees.
  - o Correct levels of access.
  - o Does everyone need access to all documents?
  - o Limit access through permissions with the minimum necessary access.
  - o Have unique accounts for each employee by name ("Ralph Smith" rather than "Receptionist")
- **Review your wireless networks.**
  - o Is your guest wireless on the same network as your medical records?
  - o Log on — Can you access your data from your guest network? (We've seen large practices with 100 employees where this occurs.)
- **Do you have an appropriate firewall?**
  - o Does your firewall actually prevent network attacks?
  - o Does it perform updates automatically?
  - o Make sure it's not an off-the-shelf $100 version from the local computer store.
  - o Fortinet/Cisco or Meraki are good ones — You need an enterprise-grade firewall.

7. Training:

Training is critical because most data breaches are caused by users who don't know better. Even smart users need reminders and refresher training. The threats come via things like ransomware — It makes its way through your users' social media or email. Criminals are getting smarter and sending realistic-looking emails, writing something that tempts users to click malicious links.

- **Your employees need to know what to click on and not,** and how to identify bad emails. How do they determine if a link is bogus or not? What kinds of passwords should they use? Do they encrypt thumb drives they take home? — And much more.
- **Call your IT provider to do this training.** They will have the most up-to-date threat info.

There's a lot more to know. It's just not possible to include it all in one article!

So, how do you keep your medical practice off the Wall of Shame? By keeping your patient data safe from cyberthreats.

Veltec Networks

Veltec Networks can help.
Contact us at (408) 849-4441, Toll Free: (855) 5-VELTEC or email info@veltecnetworks.com.