

## Medical Clinic I.T. Best Practices

Listed below are several areas within a medical clinic that should be reviewed frequently to ensure patient data is secure. By following these best practices the goal is to help prevent any data loss and improve compliance with HIPAA requirements. It is the responsibility of the clinic to take measures to mitigate any reasonably anticipated risks to protect patient health information. This document is meant to help with protection along the lines of the Physical Safeguards and Technical Safeguard requirements.

### Internet Access / Firewalls:

Internet security should be the first area to review. It is important to ensure your network is not accessible from the outside threats.

- Install and configure a Hardware firewall behind your ISP's router to protect the network from unwanted visitors and hackers.
- The firewall should provide the following features offering Unified Threat Management (UTM):
  - UTM – Refers to content filtering, Antivirus and Anti-spyware.
  - Limit the web sites your staff has access to.
  - The firewall should provide SPI (Stateful Packet Inspection).
  - Change username and password from default to have two part authentication.
  - Keep information in a safe place.

### Network Security:

Access to the network locally and over the Internet needs to be secured by complex passwords. The following password requirements should be followed.

- Passwords should be at least 8 characters in length including capitals, numbers and a symbol.
- Passwords should be changed every 90 days or if a staff member leaves the clinic that may know any of the passwords.
- Do not share passwords or usernames between staff. Each staff member should have their own username and password for their individual use only.

### Wireless Access:

Wireless access to patient information through handheld devices, tablets and/or laptops should be encrypted and secured. These 5 items will help to prevent access to your network from the outside.

- Install a secure wireless device behind the firewall only for staff use.
- The firewall must offer encryption levels greater than 128 bit encryption utilizing WPA or better. (WEP is not recommended)
- Change the login information to the wireless access point from the factory default and store in a secure location.
- Disable the SSID broadcasting so others do not see your network.
- Enable the MAC address filtering for the devices you want to have access. This will tell the wireless access point to only allow identified equipment access to the network.

## Backups:

Data backup is critical to ensuring data is not lost in the event of a system failure, disaster, or theft. Make sure all client data and important records are backed up and stored off site. There are several different options to backup data and multiple backups are also recommended.

- Tape Backups
  - Make sure your backup jobs are saved onto a tape with a two week rotation. This means you should have a separate tape for each of your work days for at least two weeks.
  - Take your tapes off site and keep secure in a climate controlled environment. A safe deposit box or fire proof safe are good options. Do not leave them in a vehicle due to either extreme heat or cold; this can damage the tape and the data.
  - Take one of your tapes each month and make a month end tape for storage up to a year.
  - It is recommended to use a backup application that can encrypt the tape and password-protect the tape as well.
- External Hard Drive
  - A couple external hard drives can also provide the same level of backup where they are changed out each week.
  - Create a daily backup for each day then make sure you have backups for each day that week.
  - Rotate the drives each week and store the second drive off site in a climate controlled secure location. Do not leave them in your vehicle due to either extreme heat or cold.
  - External hard drives can also be encrypted and should be prior to backing up data to be taken off site.
- Online backup
  - Online backup are great as long as the data is encrypted at 128 bit or higher. Data is typically compressed, encrypted and transmitted over the internet to a secure facility.
  - Make sure your encryption passphrase is secure and stored in a safe location.
  - If you lose your encryption passphrase most providers will not be able to access your data for security reasons.

## Privacy Screens:

In high traffic areas where screens can be seen by patients, it is recommended that privacy screens are used to prevent the viewing from patients.

- Privacy screens should be placed on any monitors that are at a front desk or in an exam room where EMR is utilized.
- Working in public locations or on aircraft with tablets or laptops regarding patient information it is also recommended that a privacy screen is used to protect the visibility of the screen.

## Laptop or Tablet Travel: - Encryption

Travelling with laptops and tablets has become very popular providing access to office systems and email. It is highly recommend that your laptop hard drive be encrypted to protect any data from loss or theft.

- There are several products out there that can encrypt a hard drive and render it useless to anyone who may find your computer or has stolen it. Some of these products are free and can take around 3-4 hours to encrypt.
- Encryption levels can also be adjusted with many products and it is recommended to use 256 bit AES encryption or higher.
- Always try and avoid keeping client information locally on a mobile device like a laptop or tablet if extensive travel with the device is used.
- Avoid accessing personal sites when using an unsecured wireless internet WiFi. Always use a secure VPN connection to access patient information at your offices when traveling.

## **Home Access & SSL Certificates:**

With increased utilization of RDP (Remote Desktop Protocol) connections from home back to office computers it is recommended that an SSL certificate be applied to your office network. This will make sure that the data that is flowing between the computers is not seen by hackers.

- SSL Certificates can be purchased and applied on an annual basis. The cost can range but is relatively in expensive starting around \$50.00 per year.

## **Emails & PDA's Spam Filter:**

Email services are now able to synchronize important emails with Mobile devices in real-time. Securing the emails is important and should be encrypted as well.

- Using a SSL certificate to secure your email will make sure that data moving between mobile devices is secure.
- Spam filters are also critical to maintaining a safe and secure network. By filtering out the unwanted emails prior to receiving them, will greatly decrease the possibility of receiving any viruses or Trojan onto your network or computers.
- Spam filters will also hold data if the internet at your offices goes down until restored instead of bouncing back emails to the sender. Upon restoration, emails will then be sent.
- When sending emails between clients that may have confidential information us an email encryption service. There are many out there and have several pros and cons with each type.

## **Logon / Log off:**

Setting your system to automatically log you off is a great way to protect your system from visitors or patients. If staff members walk away from their system and fail to log out prior to lunch or get pulled away unexpectedly, the system can log them automatically.

- Any time a user steps away from a terminal for a short time they should log off especially if the system is in a patient room.
- Set up an auto log off if a user is away from a system for more than 5 minutes. This will help prevent curiosity by others and keep patient information secure.

## **Anti-Virus:**

All equipment should have a current Anti-virus loaded to protect systems from outside threats.

- Keep all systems current with updated DATs to protect systems.
- Annually renew your Anti-virus with your provider or the AV manufacturer.

## **Server and Network Security:**

When at all possible keep your server and firewall in a secure well ventilated room that can be locked.

## **Disaster Recovery:**

Disasters happen when they are least expected and can cause major delays in getting your business back up and functioning. To alleviate downtime with your data take some time to identify a location that you can work from and restore your data to.

- The ability to have a snap shot of your server stored at an offsite location where you would be able to re-point another machine at a temporary location will help with the recovery.
- Take some time and work with a specialist to make sure all areas of your business can be functional at another location and review any plan quarterly.

*“Phoenix constantly exceeds our expectations in responsiveness and quality of work. Their engineers are very knowledgeable and great to work with. I would highly recommend Phoenix Technology Solutions to any business looking for a tech support company that goes the extra mile.”*

Jackie McMahon  
Clinic Administrator  
Minnesota Orthopaedic Specialists, P.A.

## What you should expect from a service partner like PHOENIX:

- ✓ Excellent products, services, and support at a great price.
- ✓ 24/7 service easily reached when needed.
- ✓ Real time documentation and communication of work completed.
- ✓ Remote issue resolution that is quick and efficient.
- ✓ System and network monitoring providing timely alerts.
- ✓ Monthly reporting that lets you know how your network health is.
- ✓ Certified engineers that can resolve technology needs quickly.
- ✓ Monthly fixed cost agreements or pay as you go services that fit your budget needs.
- ✓ Quarterly meetings to review business direction and technology requirements.
- ✓ Over 20 years of servicing the Twin Cities medical and business communities.
- ✓ Microsoft Gold Certified Partner & VMWare Certified Partner
- ✓ Professional engineers that care about your business.
- ✓ Cloud computing experts.