Data Security 101 - What Every Doctor Needs To Know

Could your business survive an attack? Are you protected?

Will your safeguards hold up? Do you know the threats?

You can…and you should. The villains are working to get in twenty-four hours a day.

Your systems should be working the same way.

The Data Security Mission: Where to start?

1. Your mission: To protect your practice data and systems.

2. Tools and strategies. Safeguards to defend yourself.

3. Find the Ally. Professionals to execute the plan.

4. Profile the villains. Know what they do and what they want.

5. Build an Action Plan. Put it in place. Go.

Protect your practice and your patients.

Start with the mission.

WHAT IS DATA SECURITY?

> *IT Security is the process and mechanisms by which computer-based equipment, information, and services are protected from unintended or unauthorized access, change, or destruction. It is of particular and growing importance in line with the increasing reliance on computer systems in most societies worldwide. [Wikipedia]*

Processes and mechanisms include the people, machines and software. These help your business function. They can be used for good or ill.

Compliance regulations demand patient data is **protected** from threats.
They require you to **protect** information against:

- the wrong people getting to it-> **unauthorized access**,
- information being changed in error or for fraud-> **unauthorized change,** and
- disaster, natural or otherwise-> **unintended data destruction**.

These are external requirements.

You also have some that are closer to your heart: protect your livelihood, your family, your work. Building a good defense will help.

The Data Security Dossier

How do you defend against threats?

Every hero has a defense. They have a strategy that foils the villain's plan.
Every villain has a weakness.

Data Security has some you can use.

The Strategies:

Updates - Software and hardware require updates.

> **N**ew threats are designed and released daily. Automated updates of threat profiles from a reputable company are standard **security** practice.

Monitoring - **Data Security** software needs someone to act when something suspicious is discovered.

> A quarantine and notification — usually an automated email or text — to <u>someone who can do something about it.</u> It says a character of interest has arrived.

Management - Both software AND hardware need regular review to stay in good working order.

> All systems are regularly updated and sized for the load they carry.

The Ally:

The *Managed Service Provider,* known as the *MSP.*

A good MSP is your best ally. They are trained IT and **Data Security** professionals hired to *manage, monitor,* and *update* your systems and software.

A professional will know HIPPA, HITECH, PCI and any other compliance regulations you are accountable for. They build these requirements into your systems for you.

You studied for years to do what you do. You hired professional practice staff. You hire professionals because you trust them.

They allow you to focus on your life.

The same is true for **IT Services.** Find your ally.

And now…(*ominous music playing in the background*)

The Villains:

Viruses - You know this one: Destructive Parasites. They destroy systems from the inside out.

They get in on files, flash drives, downloads and anything that takes a click to open.

The Tools:

1. **Anti-Virus software** provides system protection.
   Monitoring and *updates* to your **Anti-virus software** need to be applied AND recorded.

   You need proof should virus damage require insurance or law enforcement get involved.

2. A *monitored* and *managed* **Firewall with gateway anti-virus** is the fortification. It puts a wall around your network, checking all who come in and go out.

Malware - ** The terrorist cell — officially: 'Malicious Software**' : built by professional criminals targeting banking and credit card information.

A single file containing multiple offenders — viruses, spyware, ransomware, trojans, worms and other villains — which move through whole systems.

The Tools:

1. An **Anti-malware system** watches for these multi-faceted offenders.
   Updates and *monitoring* keep it strong**.**

2. **Firewall Content Filtering** captures **malware** packages at entry. Filtering requires *IT management* skills. Finding the correct balance is always worth the effort.

Hacking - The burglar. They seek **unauthorized access** to data in a system.

Not just yours but your clients' as well. And they aren't updating the Christmas list.

The Tools:

1. A solid **Firewall** that is *managed, updated* and *monitored.*
   Firewalls detect hackers trying to gain **Remote Access** to your systems.

   It's the wall around your fortress. Keep it strong.

2. Have secure **Remote Access** software.

Does anyone access systems from their home, phone or tablet? What do they use?

Use secure tools built by reputable companies. Free tools have holes and could be the hack itself.

User Error - The inside job. Sadly, it is the most common cause of **unauthorized data change and loss.**

Embarrassment, fear, tears, loss of reputation and money can come with this one. There is often no criminal intent.

This is also one of the easiest things to avoid. Most staff are honest, hard-working people.

Your mission here is simple:

- make sure staff is <u>correctly</u> **trained,**
- educate them on **risks** coming in, and
- install barriers to **unauthorized access.**

<u>The Tools:</u>

1. T**raining**. Your *Practice Management System* has its own **training**.
Make sure <u>everyone</u> goes through the **training modules** for their job.

2. Verify **user access** to your systems. Not everyone needs **access** to everything.

While it makes *user management* easy, it also leaves a door open. Intentional or not.

- Technicians don’t need patient financial access.
- Billing staff shouldn’t see patient records.
- How many people can see your payroll? Your financials?

If you’ve never done a **user access audit**, put it on your calendar <u>now</u>.

Phishing - The con man. This one looks friendly, talks fast, and gets right past you.

This guy swipes logos and layouts from legitimate companies then changes the links to point to their sites.

Once there, they download an evil minion to your machine to handle the dirty work.

- Financial institutions don't ask for password resets at random.
- The IRS does not use email with taxpayers.
- Nigerian princes do not need your help to transfer millions.

<u>The Tools:</u>

1. An **acceptable use policy.** It defines what is and is not allowed on business machines.

- Don’t check personal email.
- Be careful what attachments are opened. When in doubt: don’t click it, pitch it.

2. **Firewall Content Filtering** can spot these grifters and send them to the fortified trash bin for disposal. This needs to be *monitored, managed* and *updated.*

System Crash - A blowout, pure and simple. As with many ‘accidents’, it is highly avoidable.

Remember the 2-of-3 rule: *You can have fast, good or cheap. Pick two.*

Here we focus on *good value.* Get the best *value* for your money.

You’ll be grateful for it someday.

The Tools:

1.Buy solid, **business-class hardware** with a reputable pedigree and a valid warranty. Don't use questionable equipment. You get what you pay for.

2. Hire a **Managed Service Provider** (MSP). Your trusted ally in this mission. Professionals to get the job done.

The **Dental Integrators Association** is a good start. You can find a provider in your area and see their defined standards of service.

Natural Disaster - Acts of Nature, God or War. We live in a scary world. It is virtually impossible to stop damage from a tornado, fire or terrorist-hacker bent on destruction.

You may not be able to stop them, but you can be prepared, you can recover, and you should have a plan.

The Tools:

1. We call on the ally: the **Managed Service Provider** (MSP). We need a pro.
A good MSP will build:
   - A solid **Disaster Recovery Plan (DR) -** Your information should get regular back-ups. This keeps records safe should you need it — disaster, legal, insurance, or breach.
   - A **Business Continuity Plan (BCP) -** This plans how you will get IT systems restored to working order. How will you get back to work and how long will it take?

The Action Plan: What you can do today

Crime never sleeps. Start building your defenses:

1. Get an **Employee Acceptable Use Policy -** make some notes, talk to partners, get one started.

2. Do a **User Access Audit** - Don’t assume, verify.

3. Check your **Secure Remote Access**. Is it reputable?

4. Check with your **Managed Service Provider (MSP)** about:
   - **DR Plan** for **Disaster Recovery**
   - **BCP Plan** for **Business Continuity**
   - **HIPPA, HITECH, and PCI Compliance** safeguards

Now you have some skills, defenses, and allies. You have tools and knowledge. Use it for good.

“***With great power comes great responsibility.”***
— Peter Parker’s Uncle Ben in Spider-man

Stop the villains in their tracks.

Be your own superhero.