Top-10 Ways to Lose Critical Data

The safety of your data is critical to the success of your business, not only because of laws such as HIPPA, HITECH and PCI, but to protect the safety and privacy of your patients that trust you with their information.

Below are the top-10 most common ways that data gets lost:

1. **Malware.** This is that nasty and malicious software that you can accidentally download onto your computer systems if your internet security software is not up to date.

2. **Hackers.** Medical information is a prime target for hackers, who will sell your customer's personal medical information to criminals who then use it to perpetrate fraud. The most common vulnerability is a poor internet firewall.

3. **Inadequate Passwords.** Simple passwords (short with no alpha / numeric / upper case characters) are easy to crack. Beyond that, sharing passwords or posting them on a sticky note near your keyboard is asking for trouble.

4. **Failure to back-up data.** Losing your data is the worst possible security breach of all. Backing up your data to a cloud-based solution is easy and automatic.

5. **Improper use of Social Media.** This is a growing security risk. Internet attacks, fraud, and Malware launched onto your network via innocent looking emails and careless social media surfing can cause damage or loss. Have a social media policy that makes sense, and train your employees on the risks.

6. **It's not just about electronically stored information.** The physical protection of your client's data is just as important. One of the largest data breach settlements from last year ($1 Million) was paid by a company whose employee left 192 medical files on the seat of a commuter train. Remember to safeguard your physical files as well.

7. **Lost or stolen laptop computers.** Ever go out to dinner and leave your laptop in your car? Don't. Think about what is on your laptop; customer data, financial data, tax returns, irreplaceable photos. Keep your laptop secure, back it up, password protect it and use encryption.

8. **Data in Transit.** Electronic prescriptions, electronic payroll, on-line banking transactions and other data in transit can easily be intercepted if you are not using encryption for the protection of data in transit. Also, make sure your wireless router is not visible to outsiders and that its settings are secure. Remember, banks are not always responsible

for customer funds lost to fraud if their security measures were reasonable.

9. **Loose lips sink scripts.** Your client data is highly regulated by HIPAA and other laws. Remind employees to only share sensitive patient data with those with a legitimate need to know. Does your employee training process include information security awareness? It should.

10. **It's 10 O'clock, do you know where your dumpster is?** Some of the largest fines levied against pharmacies in the last few years were related to confidential patient information

Source: Cardinal Health Security Literature, Jeff Hartman with eDiscovery Lab

**The information provided should be considered as precautionary and does not warrant or represent that by implementing such measures, your business will be free from any and all security risk or damages due to criminal conduct.*