GSG
Computers
Bullet Proof Your Technology

HIPAA TIP:

6 Simple Steps to Reduce Your Risk of a Data Breach

By Lisa Good, HCISSP

1. Conduct a yearly risk assessment

In accordance with the HIPAA Security Rule, which establishes national standards to protect individuals' electronic personal health information, a thorough and accurate risk analysis must be conducted annually to assess "the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the organization."

Don't be lulled into a false sense of security because you think your practice is too small to be a target for hackers. Crimes happen most often when there is opportunity — it is easier for hackers to target a small practice and steal patient information for identity theft or credit card numbers, than it is to, say, break into American Express.

Industry studies have found that healthcare data sells for 10-20 times as much as credit card data on the black market ($10 to $20 for a health record vs. $1 to $2 for a credit card number).

Here is an interesting cybercriminal fun fact:
Pieces of health information are also sometimes combined with other pieces of data and sold on the online black market, where they can fetch $1,000 or more when bundled with counterfeit documents.

2. Enable MDM tools

Let's face it, in today's fast paced environment it is almost impossible to keep all data off of mobile devices. Securing mobile devices is as simple as investing in a mobile device management (MDM) tool. This should be on all employee devices and will provide an extra safety net in case employees' mobile devices are ever stolen from a home, office or vehicle.

Not only can MDM tools possibly protect electronic records from being accessed on mobile devices, but they can also locate those devices and allow for remote data removal (the device to be wiped) if they're lost or stolen from an employee.

3. Encrypt data and hardware

From 2009 to 2015, the loss or theft of unencrypted portable devices was responsible for more than a third of all breach incidents. The cost to encrypt a hard drive is roughly $300 per year per device, and continues to decline. When you weigh the cost of encrypting data on all portable devices and computers, it is much cheaper than the fines that would be imposed if you had a breach incident and your computers were not encrypted.

4. Monitor emails, texts and social media

Practice employees who peek at high-profile patient medical records out of curiosity may open your practice up to HIPAA fines. Since we live in a world of instant gratification (which includes instant venting), an employee may act without thinking and post something sensitive – either vague or specific – on Facebook, Twitter, etc. or send it to a friend outside the practice through a text or email. Ensure your practice is HIPAA compliant by advising employees to not post anything on social media or send an external email or text to anyone about anything that goes on in the practice. They should also know, in writing, before an incident takes place what the consequences of such actions are.

5. Don’t make changes to your network if you don’t know what you are doing – Find qualified IT Support

One of the largest HIPAA fine was issued to New York Presbyterian-Columbia, to the tune of $4.8 million. What happened demonstrates how technology and human error can combine to cause a security disaster. The short version is that a doctor attempted to deactivate a personally owned computer that was connected to the health system’s network. Because that network was configured improperly, he inadvertently exposed a large volume of PHI to open web access.

Most small to mid-sized practices don't generally have an IT budget, so they tend to gravitate to free tools, solutions, and doing things themselves, which can be catastrophic. One of the best ways to protect your practice is to find professional IT support that you can trust.

Quick tip: When evaluating an IT Support Provider, give them this quick 3 question quiz – but it has to be done orally and preferably in person.
Question 1: How do you spell HIPAA?
Question 2: What does it stand for?
Question 3: What is the difference between HIPAA security and HIPAA privacy?
If they can't answer those three questions without hesitancy then you should keep looking or you will probably have a HIPAA problem waiting to happen.

6. Provide ongoing training - Stay updated on HIPAA requirements

Maintaining compliance with HIPAA (for PHI) and PCI-DSS (for payment card data) means that you are doing your very best to keep your patients' valuable information safe and secure and out of the hands of people who could use that data fraudulently.

Educate new employees and re-educate seasoned employees on current HIPAA rules. Keeping security top-of-mind for employees reminds them of what constitutes a security breach and helps protect your practice.

Your staff training should cover at a minimum:

- The use of practice computers for personal emails and internet surfing
- Transporting data offsite using mobile devices
- Protocols for departing staff members, e.g. changing passwords & network access
- Educating staff on HIPAA requirements
- The use of mobile devices at home and work
- The consequences for not adhering to your practices policies

GSG provides employee training materials and either annual or semi-annual (depending on your practice size) security lunch-and-learns for client's employees. We make it easy to keep your employees up to date.

For questions on HIPAA compliance, employee training or how to protect your office, visit www.getbulletproofit.com/healthcare or contact us at 615-826-0017.

About the Author:
Ms. Lisa Good has over 20 years of experience in the healthcare and information technology industries. Lisa has been working with small to mid-sized practices to help them become more efficient, secure and compliant ~ long before it was popular to be on the "HIPAA" band wagon. She works relentless to help practices put solutions in place that meet the needs of their individual practice and meet the Department of Health and Human Service Guidelines as well as the HITECH Act.