9 REASONS COMPLIANCE DOES NOT MEAN YOUR PRACTICE DATA IS SECURE

WHO WANTS TO SEE YOUR PRACTICE DATA?

It feels like a throw-back to the dire predictions of George Orwell's "1984," with its now timely warnings that "Big Brother" is watching. As the digital world grows in acceptance and accessibility, it brings along associated opportunities for misuse.

Cyber security is in the forefront of evening news reports as infiltrations are discovered on an alarming basis. Everything from political parties, major retailers and financial institutions to internet giants like Facebook and Yahoo can make juicy targets. Even the U.S. government is not immune from attempts to obtain unauthorized access. According to a 2018 report from the Government Accountability Office (GAO), "nearly all of the Pentagon's newest weapons are vulnerable to attack."

The snooping and prying has not eluded the medical field. According to Healthcare IT News, "Healthcare continued to be a lucrative target for hackers in 2017 with weaponized ransomware, misconfigured cloud storage buckets and phishing emails dominating the year." Some headlines about healthcare hacks in 2018 included:

- CMS responds to data breach affecting 75,000 in federal ACA portal
- Two phishing attacks on Minnesota DHS breach 21,000 patient records
- 3 Massachusetts hospitals fined nearly $1 million by OCR for HIPAA violations
- Employee error exposes Blue Cross patient data for 3 months
- 1.4M records breached in phishing attack
- Ransomware attack breaches 40,800 patient records in Hawaii
- 417,000 Augusta University Health patient records breached
- Canadian pharmacist fined for routinely accessing health records of acquaintances
- Third-party vendor error exposes data of 19K patients for 2 months
- And the list goes on and on…

"Nearly all of the Pentagon's newest weapons are vulnerable to attack."

—GAO 2018

These attacks target valuable data that can be used for other purposes, seek to wrest ransom out of organizations that rely on quick access to information, or blatantly try to cause harm or seek revenge.

As a small medical practice you might think, "Who would want access to our information when there are so many bigger fish to catch?" But your practice has information on thousands of patients, and you might be surprised to find out that lots of people are eager to dig into those files. Their reasons vary widely from simple snooping to identity theft, prescription scams, tax fraud, and false Medicare/insurance claims.

Even if you agree that others want to obtain unauthorized access to your patients' Protected Health Information, or PHI, you could believe you have taken the necessary precautions to keep your practice data secure. Although you might even be in compliance with HIPAA guidelines, this Knowledge Drop will expose some of the simple and shocking ways data can be compromised.

WHY SHOULD MEDICAL PRACTICES CARE ABOUT CYBER SECURITY?

There are many reasons why your medical practice should care about cyber security. Most importantly, HIPAA compliance requires you to protect patient information. According to Medical Economics:

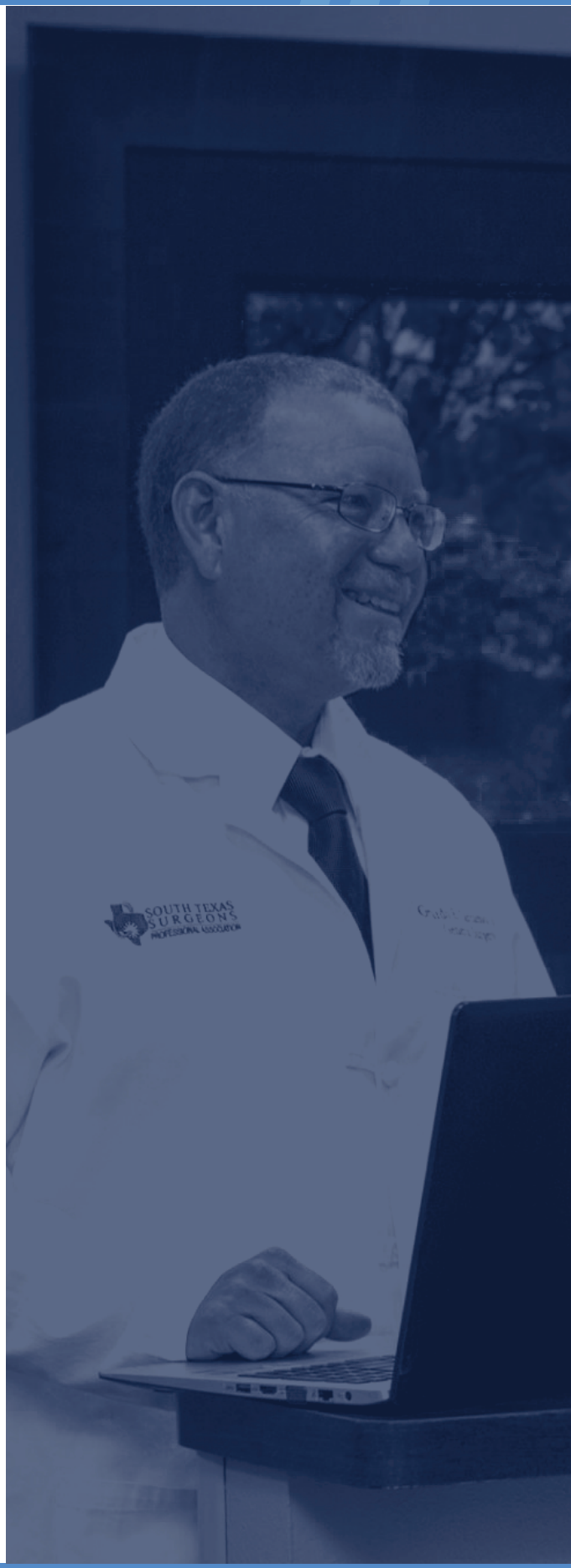
- The Privacy Rule protects individually identifiable health information in any form, whether electronic, paper, or verbal.
- Each entity must conduct a Security Risk Assessment (SRA) to analyze the risks to e-PHI in its environment and create appropriate solutions. An SRA is especially important to practices which participate in the Merit-based Incentive Program (MIPS), as part of their Promoting Interoperability requirements.
- The HIPAA Breach Notification Rule requires providers to notify affected individuals, HHS, and in some cases, the media of a breach of unsecured PHI no later than 60 days following its discovery.

Secondly, protecting patient information is a moral and ethical imperative. You want patients to trust you as a medical care provider, and they need to know information they provide is fiercely protected. Attacks on their personal data can lead to embarrassment, financial difficulties, and increased stress.

Finally, it makes good business sense to protect practice data. Data compromises can diminish your ability to provide quality care, cost your practice untold financial outlays, and irreparably damage your reputation. From the moment you realize there is a breach or receive notification from a law enforcement institution that your data was compromised, you are under constant pressure to inform patients and insurance companies at the same time you are working to resolve the situation.

If an attacker takes over your computer system in a demand for cyber ransom, you may no longer be able to access patient data to provide necessary care or write critical prescriptions. If you resolve the matter, you may be under the threat of lawsuits or insurance claims that eat up your time and financial resources. Practices found to be negligent in protecting patient data may also be subject to substantial fines and penalties.

Having a cyber-security plan is critical to the long-term functioning of your medical practice. Breaches are here, and they are accelerating. It is unwise to assume your practice is somehow immune from prying eyes that want access to private patient data.



9 REASONS WHY COMPLIANCE DOES NOT MEAN YOUR PRACTICE DATA IS SECURE

When HIPAA first appeared, medical practices were up in arms because they had to lock file cabinets and take down patient pictures – well, those were the easy days. Now, even though you have done all you can to increase cyber security, here are nine shocking reasons your PHI might be vulnerable:

1. Phishing

These strangers want access to your computer. Usually the process starts with an innocent-looking email which might say that it is from a reputable company, or it could be an obvious fraud. If someone in your practice opens this email, the sender can then install a virus or malware that starts doing its dirty work. Maybe it copies passwords, or follows private email communications, but the objective is to obtain valuable information to use for negative purposes.

2. Hacking

These targeted attacks look for ways around existing cyber security measures – this is an all-out push to gain control. You might not recognize that an attack has occurred for months, or you might discover that none of your devices work and you need to pay a "ransom" to have access restored.

3. Digital Devices

You may have protected the main computer, but what about the laptop or iPad you use to take notes? Do members of your office staff communicate with patients on personal devices, or use flash drives to transfer information? Take a look around your office and you might be surprised at the number of ways outsiders can attack your information. It's not just the computers either – connected copiers, fax machines, scanners, and printers all make great hacking targets.

4. Trusted Sources

As you work with outsiders to keep your practice running, you build trust and innocently give them access to computer passwords. It might be your IT guy, the repair technician, or an advisor, but once they have access there is no telling where they might stop.

5. Oversights

Being vigilant can be a hassle, so employees might find ways to work around security protocols. One common oversight is a password that uses the practice name, or a sticky note with the password that hangs over the centrally-located keyboard. Anyone walking by can snap a quick photo, and there goes the security you worked so hard to establish.

6. WiFi

WiFi is a great way for others to get into your system as well. Be aware of cyber threats if your practice relies on WiFi to run computers or other equipment.

7. Patients

Patients are often the least concerned about their own privacy. Keep a careful eye on patient portals and explain the importance of security when logging in or sending messages. Even fitness trackers that send information or track health data and share it with others can be easily compromised.

8. Malfeasance

This involves an employee who purposely seeks to obtain information. That person might be mad and trying to get even, it could be a criminal activity to sell data to support a vice, or they could try to harm a friend or family member by attacking their personal information.

9. And, finally, a word on employee snooping…

THE DANGERS OF EMPLOYEE SNOOPING

It seems innocent – a care provider or employee uses the office computer to check a test result without going through the patient portal, or looks up information for a family member. It may be more curious than nefarious – a neighbor has an appointment, and the employee wants to know why. It might even be to seek information to use in a legal proceeding. In any case, if access is not specifically authorized, it is a data breach.

Anyone not performing a specific treatment, office function, or healthcare operation as part of a job requirement is not authorized to look at any PHI without specific patient authorization – even for their own records or those of a family member. According to the medical data security experts at SPHER:

> **"There are few to zero instances where an employee or credentialed user should ever be examining their own medical health record. They definitely should not being 'looking' at the health record of a relative or neighbor to satisfy some curiosity. Snooping is a HIPAA violation and should be documented and reported."**

Ways to detect snooping include looking at access times, matching last names, personal record access, or patient time span. Once identified, the action needs to be addressed with the employee, with consequences based on the severity of the action. As employees realize your practice is serious about security these incidents will probably decrease, but you still have to instill this discipline as new employees are brought on board.

If a substantial breach of PHI is demonstrated, there is a high probability that some type of audit will be initiated to determine how the breach occurred and how extensive the damage to privacy is.

IMPROVING CYBER SECURITY

Steps your practice can take to improve cyber security include:

- Perform a Security Risk Assessment to look for vulnerabilities.
- Document all security protocols.
- Improve security procedures including longer passwords and two-step authentication.
- Implement constant staff training and awareness.
- Allow access only to credentialed users.
- Regularly monitor and test all devices.
- Perform an annual security audit.
- Maintain constant vigilance.
- Require all business associates to provide SRAs.

An ongoing sense of awareness is the best line of defense in the effort to maintain cyber security.