EMRSOAP
Advancing Healthcare Via Smarter Information Technology

HEALTH IT SECURITY AND THE SMALL PROVIDER

A Primer for 2013

Ben Watts

EMRSOAP 2800 156TH Ave SE Suite 100 | Bellevue WA 98007

Table of Contents

Summary

The healthcare industry currently faces wide security risks and will either become more responsive and secure, or face penalties. On the whole, the industry is vastly undervaluing the data it possesses, leading to small security budgets and inattention from management. Avi Rubin, Computer Scientist and Director of the Information Security Institute at Johns Hopkins University, said, “I have never seen an industry with more gaping security holes…if our financial industry regarded security the way the health-care sector does, I would stuff my cash in a mattress under my bed.”[i]

Often having the least capacity of their sector, small healthcare practices are especially at risk. Because of weak enforcement, lack of attention being paid to smaller providers, and the difficulty and expense of security and compliance, they have understandably neglected ePHI[ii] security and HIPAA compliance. However, several structural features have changed over the past year, leaving small provider practices vulnerable.

This paper seeks to **educate the Small Provider Practice on the changing Health IT compliance and security landscape**, and **arm them with the information to make better Health IT decisions**.

Why should a Small Provider care about protecting ePHI?

1. *It’s the right thing to do.*

From the moment a patient walks in the door, they are placing vast amounts of trust into a medical practice’s hands. In recognition of that trust, Doctors swear oaths to treat their patient ethically and honestly.

A patient’s trust extends to how the practice handles their data. Practices are handling sensitive information that can severely damage an individual’s reputation or financial standing. Imagine if a list of HIV-positive patients got onto the internet, or if an employer could discriminate against a potential employee based on a detailed medical history. If a patient’s medical identity is stolen, it can be a problem that lasts over a decade to effectively solve, as they would have to address each incorrect record on a case by case basis.

In Short: the process of caring for patients will be degraded if they lose trust in their providers. In order to protect patients and make their practice worthy of trust, small healthcare providers should do their part in protecting their patients’ ePHI.

2. *ePHI is a business asset. It should be protected like one.*

ePHI is crucial for the continuance of a practice’s success. Electronic systems increase billing, help manage patient care over time, and increase the efficiency of healthcare workers. Rather than spending minutes (that turn into hours) deciphering handwriting, looking for charts, or examining archival records, a caregiver can access information in a matter of clicks.

However, for all the benefits that electronic systems bring, they also include potential problems. If a practice fails to adequately protect their ePHI systems, it can be disastrous. Imagine if all a practice's records were lost simultaneously, or were corrupted – how would you react? Would your business be able to continue serving patients?

In December 2012[iii], a practice in Australia failed to protect their backups, to terrifying effect. A hacker, likely from Eastern Europe, broke into the Miami Family Medical Centre's IT systems, encrypted all their ePHI, and held it for ransom. Experts say that it's probable that the Medical Centre will never get their records back. This is not an isolated incident – in 2012, similar occurrences happened in the US.

In Short: Just like a lock on the front door, investing in IT security is a necessary investment for a small provider's continued business success.

3. *Protecting ePHI will save you money in the long run.*

We'll go into this in greater detail below, but not protecting your patients' ePHI can be extremely costly.

If a significant breach[iv] of ePHI occurs, your practice will have to scramble very quickly. Micky Tripathi, CEO of Massachusetts eHealth Collaborative, has written an excellent blog[v] post about a firsthand account of a breach. We recommend reading it.

By his own accounting, it cost his company $288,808 in hard costs – the economic opportunity cost of 600 hours of his staff's time was not accounted for. This was for a breach of about 1000 patient's records – and his company was not even fined by any government entities.

In Short: By proactively protecting your practice, you can avoid thousands of dollars of costs down the road. Spending money on IT security might be painful, but it's a worthwhile part of protecting your business.

Is my practice currently in danger?

It is very likely that the answer is yes. In this section, we'll be examining the various sources of danger that your practice is facing.

1. *Malicious Hackers*

As already detailed above, Hackers are out there, and patients' ePHI is valuable target. Even if you don't find yourself holding a blackmail letter and a hard drive encrypted by a criminal, hackers can still profit off of your lax security.

Just how valuable is ePHI to a Hacker? To put this in perspective: a medical record is worth $50 on the black market, while Social Security number is worth $3, and credit card information is worth $1.50. If they get 5,000 records off of your system, that's worth $250,000 to them. [vi]

In Short: Hackers have a real incentive to attack your systems. Ignoring them won't make them go away.

2. *Increased Government Audits*

From all sides, government regulation of the Healthcare industry looks to be steadily increasing over the next few years.

State Regulations: State Attorney Generals were trained in 2011[vii] about how to enforce HIPAA, and we've since seen an increase in state-level enforcement of HIPAA.

HIPAA Audits: OIG, the office the polices HIPAA, is currently evaluating it's HIPAA audit process, but they'll be done by the end of the year. During the initial audits, the smallest type of provider was 20% [viii]of the audits – leaving little room for the belief that small providers won't get noticed.

Procrastinators might consider that they won't have to implement any changes until the new audit start. While this is a creative idea, it won't work – the audits demand proof of your ongoing, historical compliance. Continually delaying will make your life incredibly difficult in the event of an audit.

Meaningful Use Audits: If your practice is seeking to attest to Meaningful Use, the government incentive program that rewards the implementation of an Electronic Medical Record program, it will need to complete a Risk Analysis, the beginning process of protecting your patient's data. Currently, the attestation process trusted providers that they had completed a Risk Analysis.

However, increased political pressure from oversight organizations[ix] suggests that the attestation process will increase in difficult in the future. It is likely that attesters will have to submit extensive proof of a Risk Assessment before receiving any money.

In short: Small providers can expect increased government regulations for lax security and compliance.

3. *Inevitable ePHI Breaches*

Taking an ‘it won’t happen to me’ stance is a losing position. Breaches are entirely too likely to occur: 27% of responders of a HIMSS survey[x] reported that their organization suffered an ePHI breach in the previous year.

Breaches can happen over a wide variety of vectors. Here is just a short list:

- A virus could enter your ePHI systems, sending it to an outside party
- A Business Associate that you give ePHI to could have a breach of their own.
- An unencrypted backup drive is stolen from an employee’s car
- An employee could fax someone’s ePHI to the wrong party.
- An employee could snoop into a ex’s or Celebrity’s ePHI when they have no medical need to do so.
- An disgruntled employee could steal patients’ information to sell on the black market.
- A recently fired employee could return to the office to steal a hard drive to hurt the company.
- An office kitchen fire could set off your sprinklers, soaking all your backup hard drives at once.

2012 was the first year that a small provider was fined for a breach. Phoenix Cardiology, a 5 physician practice, was fined $100,000 for publicly releasing their calendars full of ePHI onto the internet, as well as being completely out of HIPAA compliance. Leon Rodriguez, head of OCR (the regulators of HIPAA and ePHI breaches), said that ‘every one of [these cases] is a message to the rest of the industry’. Later, he explained that message even more, saying that ‘OCR expects full compliance no matter the size of a covered entity.’

Government regulators will not regard a small providers’ size as a deterrent in issuing fines. More and more, the healthcare industry, including small providers, will be facing increasing monetary enforcement.

In Short: small providers will increasingly be subject to large regulatory fines for breaches of ePHI. Unless proper safeguards are implemented, breaches are an unfortunately common occurrence.

What are my next steps?

Rather than overwhelm you with a giant list of steps required for sufficient security and compliance, we're offering 3 significant steps that will put you in the right direction.

1. *Give Health IT Security and Compliance the consideration it requires*

A main reason efforts to become secure and compliant fail is that management did not provide enough support. In order for your organization to actually remove the risks associated with poor security, it needs full financial and management support. After all, major organizational changes have to occur in order to become secure – without management, these changes often do very poorly.

Make sure that top-level management is included in discussions about IT Security and HIPAA compliance. Don't give implementers a shoestring budget. Ensure that enough support is given to actors making organizational changes.

2. *Develop a route to Health IT Security and Compliance*

Who on your team will oversee this process? Do you have competent IT support for this task? Is your IT personnel trained in HIPAA, data security, backups, and other required specialty fields?

Most small practices will struggle to fully implement Health IT Security and Compliance – the specific requirements of Risk Assessments, HIPAA, and quality IT security are often beyond the in-house resources that a small practice has. Dumping even more work on the office manager is not a sufficient plan.

Relying on a qualified Health IT consultant is often a good way to compensate for these problems. However, make sure that they are used to interfacing with small practices – as their needs are greatly different than larger institutions.

3. *Complete a Risk Assessment*

Not only is it required by law, but a Risk Assessment is the first serious step towards security. Without it, your practice could be facing any number of dangers without being aware of them. A proper Risk Assessment is a complex process - make sure that it complies with NIST guidelines.

Conclusion

The IT environmental landscape around small providers looks vastly different this year. They are under increased regulatory pressure, and can face significant damage to their practice if they do not increase their IT security.

EMRSoap is prepared to help small practices manage their IT security and regulatory compliance. With experience work with numerous types of practices, and with a specialty in implementing changes in small practices that make sense for their specific organization, we can help your organization navigate the complexities of the coming regulatory oversight.

EMRSOAP
Advancing Healthcare Via Smarter Information Technology

References

[i] http://www.washingtonpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html

[ii] Electronic Patient Health Information – health information that links to information that can be used to identify an individual.

[iii] http://www.abc.net.au/news/2012-12-10/hackers-target-gold-coast-medical-centre/4418676

[iv] HHS defines a breach to be: "Generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual."

[v] http://www.histalkpractice.com/2011/12/03/first-hand-experience-with-a-patient-data-security-breach-12311/

[vi] http://blog.veriphyr.com/2011/12/cost-medical-identity-theft.html

[vii] http://www.govhealthit.com/news/ocr-will-train-state-ags-enforce-hipaa

viii http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-2_lsanches_ocr-audit.pdf

ix https://oig.hhs.gov/oei/reports/oei-05-11-00250.pdf

[x] http://www.krollcybersecurity.com/media/Kroll-HIMSS_2012_-_Security_of_Patient_Data_040912.pdf