ControlScan

SECURITY    COMPLIANCE    ABOUT    KNOWLEDGE CENTER    PARTNER PROGRAMS

# Securing Patient Data: Where should your healthcare organization begin?

Strong patient data security starts with the help of five key team members.

Home / ControlScan Blog / Securing Patient Data: Where should your healthcare organization begin?

September 26, 2016 • Published by Kim Carlos

Cloud Security • Ransomware

## There's a state of emergency within patient care.

If you're in healthcare, there's probably no need for me to sit here and tell you about all the problems you are currently facing with patient data security. You've heard it, you've read it and you're experiencing the pressure daily.

Historically security has played second fiddle to regulatory and usability demands within the healthcare industry. So, what's changed? It seems like everything: Rapid digitization of healthcare records, incentives for meaningful use, deployment of network-connected devices to make monitoring more efficient, bring-your-own-device (BYOD), increased competition, demands from patients for top-notch care—the list goes on and on.

The problem seems so large, complex and expensive that it's easy to feel paralyzed. There's plenty of bad news and blame to go around. But, how do you find your way through a problem that seems so daunting?

## You need people to fight people!

Staying ahead of hackers and other threats to your organization really is a full-time job that takes more than just implementing the latest technical safeguard. You need people to fight people.

As we've seen recently with healthcare ransomware attacks, there are more and more daily attacks on patient care facilities, and the malware used continues to become more sophisticated. In addition, PCI DSS and HIPAA/HITECH compliance each play a huge role in the healthcare industry, so much so that "complying" can become just as important as actual healthcare data security.

Establishing a strong foundation of security and compliance involves surrounding your business with the right team of people:

+ **An engaged C-level executive** – Support for your organization's security and compliance should come from the top. Even if this person isn't a security or IT expert, they should understand and have visibility into all security-related technologies, processes and policies.
+ **A compliance guru** – Someone within your organization that understands all the HIPAA and other regulations that need to be met with any technology platform you put in place. This is actually a required position in HIPAA and often carries the title of Privacy Officer. Some organizations have a compliance officer and privacy officer or combine the roles. This person has a lot to offer, so be sure to stay open minded and listen to their input.
+ **An IT security champion** – Someone who is willing to lead the team during both the research and implementation process. It's important that this person is included from the beginning. This person does not have to be a security expert, but an IT background is a must.
+ **Process improvement streamliner** – This member is the one who loves putting processes into place. In healthcare, it's often someone with administrative duties who knows the ins and outs of your business. Because a "set it and forget it" mentality just isn't realistic with cybersecurity, this person's perspective will help you see holes that you might not otherwise be aware of.
+ **Security operations expert** – This is the person that will be ever vigilant in watching all of your 'doors' to ensure no one is trying to sneak in. This is the person that is often missing internally from the small to mid-sized business due to lack of budget or scarcity of the supply. If you don't have a SecOps expert internally, this is a partnership you can outsource and save money.

## How to fill the security people gaps?

It's a big problem, so where do you start? Hopefully your organization has an engaged chief

---

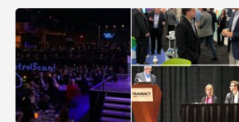**Tweets** by @ControlScan

**ControlScan**
@ControlScan

We had a fantastic week meeting and exchanging insights with both longtime and brand-new friends in #payments at #ETATRANSACT! Thanks, @agzirkle and @ETATRANSACT, for all the hard work you put into producing this high-caliber industry event.

May 3, 2019

**ControlScan**
@ControlScan

It's the final day of #ETATRANSACT! Here's Tom Callahan (@tomtheitguy), Director of Operations at our Hunt Valley, MD Security Operations Center, modeling our sweet t-shirt! Come by booth 2912 and get you one. #SOC #MDR

executive (*if not, share this post with them!*), but if the other individuals I've outlined above aren't a feasible hire, you may want to consider partnering with a managed security service provider (MSSP). Not only can an MSSP be a cost-effective alternative to one or more full-time internal resources, they can also help implement and maintain your security technology infrastructure.

Partnering with the right expert really is the "easy button" for organizations of a particular size. If you are looking for a quick way to get the ball rolling, start with a risk assessment, as it is usually the first step toward HIPAA compliance. Ensuring patient data is secure is the only way to truly provide patients with the total-care experience that they now require. If you don't, someone else will and a patient will likely follow the path that looks the safest.

## Tags

Access Control Active Monitoring Cloud Security Compliance Cybersecurity Legislation EMV Encryption Endpoint Security Firewalls Internet of Things Malware MDR Mobile Security Network Security Payment Security PCI Compliance Physical Security Point of Sale Ransomware Security Assessments Security Awareness SIEM Social Engineering Vulnerability Management Website Security Wireless Security