How One Organization Successfully Implemented a HIPAA Security Program

August 8, 2019

Proteus Consulting performed a risk analysis earlier this year for a company that we initially assessed and began providing programmatic coaching in 2017. We are omitting the company's name for obvious reasons. Prior to our first encounter, this company's ability to demonstrate Health and Human Services compliance was inadequate and mainstream security technology controls were employed to protect their electronic protected health information (ePHI). More important was their vulnerability to an expensive Office of Civil Rights corrective action plan. As a result of their work and regular communications, their 2019 risk analysis that included *an evaluation of 181 vulnerabilities yielded only three risks* into their current risk register.

It would be arrogant to state that our client simply followed our recommendations. What follows are two key factors that enable their accomplishment. HIPAA Security Rule compliance and the ability to safeguard ePHI is a journey – not a destination – and you too can enjoy similar success.

The Importance of Company Culture

We recognize that many organizations struggle with their compliance programs, at least partly due to a lack of commitment by their leadership, to see ePHI security beyond a general liability. We also acknowledge that many decision makers are broadly aware of ePHI security, but fail to resource it as other business requirements.

In this case study, the executive leadership team had set expectations to act ethically for all of their business functions long before we met. Protecting patient privacy is not just a marketing slogan, it's a commitment backed up by action. Computer session timeouts and screen savers are not seen as a productivity hindrance; rather, as help when a workstation is accidentally left unused for a period. Second, this company demonstrates a desire to do the work required and to overcome learning curves associated with new information or processes. Realizing that everyone already has more work than time in the day, their team makes adjustments to their other tasking to fit HIPAA security into their week. Their character and company's guiding principles are reinforced from the individual caregiver, through support-services staff, to their c-suite.

The Takeaway?

It is possible for a HIPAA Security Officer to run a compliant program that employs reasonable and appropriate ePHI security controls. This program is made easier when everyone works from the same vision, when each team member makes time for one another, and when information security controls and understood and deployed.

The Importance of Accountability

Program sponsorship is something we emphatically recommend to all of our clients. Sponsorship means that someone on the senior leadership team (preferably in the c-suite or a VP) is in tune with the program, provides the resources to accomplish the work, and verifies the program's value as it relates to the company's mission or vision.

Our case study company sought out and secured a VP-level program sponsor. As they were already monitoring medical operations risk, their team leveraged experience coordinating other enterprise processes to support their (new) program. Resourcing the program was the first challenge that the sponsor helped solve, as many of the company's services are tethered to a funding revenue stream and no one source was meant to fund regulatory compliance. The program sponsor chairs monthly meetings, where she maintains an active role listening to the program's challenges and providing guidance to the team. She recognizes that "phantom-sponsorship" won't work.

Each member of the HIPAA team also holds each other accountable. The HIPAA Security and Privacy Officers chair a PHI risk board that meets monthly; in between meetings these two positions regularly share their privacy and security incidents, and co-draft periodic security reminders. Other members include identified information owners, who in this case are the workforce members overseeing or administering their ePHI systems, and information technology representatives. As this board established itself, they focused on the nine PROTEUS Security Rule policy and procedure documents and created "to do" lists, beginning with the easier-to-accomplish tasks to create the momentum to sustain the more challenging discussions. Interestingly, risk mitigation was important, but was focused on after the team better understood the technology-based terms. Their board inclusion strengthened the information technology team's partnership and helped the organization better understand the need for technical projects previously not implemented.

Lastly, each team member also holds themselves accountable to create and sustain a program earnestly invested to protect ePHI. As one of many examples, the information technology team we encountered is simply outstanding. Not only were we impressed with how few of them exist, but in their ability to keep abreast of and implement current technology. They push themselves to learn what technology company grants and discounts exist and they earn certifications beyond what is required to perform their daily job.

The Takeaway?

We recognize that not every HIPAA Security Officer has the luxury of a program sponsor or the ability to untangle a multi-revenue stream to base a program. But the real work is being done far below the front office and people can focus themselves and their teams and hold each other accountable in a positive way that promotes the program objectives.

Conclusion

Covered Entities and Business Associates share the same HIPAA Security program challenges. This whitepaper discussed two best practices to improve program effectiveness, reduce ePHI risk and protect the company from the financial consequences of an unauthorized disclosure event (i.e. an ePHI breach). We realize that some programs may not be able to manage themselves as formally and we encourage compliance officers to integrate these recommendations as much as company culture will permit.

The challenges of regulatory compliance are overt and require effort to demonstrate a reasonable and appropriate program. Protecting ePHI is integral to modern patient care and to the healthcare community's reputation. Realizing how HIPAA is administered and acknowledging limitations, whether they be fiscal- or employee expertise-based, can frame a healthy discussion and provide productive direction that improves patient outcomes, decreases operational risk, and protects the limited financial space most healthcare organizations operate under.

HIPAA Security program compliance is achievable. A key component is putting the right people in the right positions to enable the best outcomes. Often, very bright and capable people are in the wrong seat and this unknowingly blocks success. You've got an experienced partner in Proteus Consulting dedicated to your program's success – let us know what help you need.