Going Beyond HIPAA: Digital Health Risk Management and Cybersecurity

Data breaches in healthcare have garnered headline after headline in recent months. Not surprisingly, then, with the problem gaining so much attention, data security and privacy has become a growing concern for healthcare executives.

Recently, enterprise cybersecurity expert Shahid Shah, also known as “the Healthcare IT Guy,” addressed the many challenges associated with keeping healthcare data safe during “How to Move Digital Health Cybersecurity Beyond HIPAA Compliance,” a webinar sponsored by Iron Mountain and presented by Health Data Management magazine.

During the webinar, Shah offered some tips and advice. In fact, the well-known speaker challenged the commonly held assumption that data security in healthcare is different than it is in other industries and, therefore, requires unique protection strategies and tools. Instead, Shah proposed that healthcare organizations implement the strategies and tools that are used in other industries and promulgated by organizations such as the Department of Homeland Security (DHS), Department of Defense (DOD) and National Institute of Standards and Technology (NIST) to create comprehensive security and privacy initiatives.

The State of Data Security in Healthcare
Greg Slabodkin, managing editor of Health Data Management and the moderator of the webinar, opened up the presentation by talking about the current state of data security in healthcare. He specifically pointed to the significant number of healthcare data breaches that have been reported on in the news recently.
With all of this upheaval and so many data challenges prevalent in the healthcare industry, it’s not surprising to find that many healthcare organizations are seeking to implement healthcare-specific solutions to mitigate their data security risks. But, taking this very healthcare specific approach might lead organizations down the wrong road, according to Shah.

“"A lot of healthcare institutions, whether it’s payers or healthcare providers or others, are... thinking that there’s something special about healthcare data security and they are looking for [specific] healthcare data security and data solutions. But they are going to find that they’re going to be quite limited,” Shah said.

While it might be important to understand why healthcare data is different, it’s more important to comprehend why healthcare security programs need to mirror those found in other industries. Shah pointed out that healthcare leaders should “understand [their] data, how it’s structured, why people would want to steal it, what it is valued at, etc. But when [they] look at tools and approaches and technologies, [they] need to do so in a way that is much broader so that you can get the best help.”

Moving Beyond HIPAA

Indeed, Shah stressed that when taking the "healthcare" approach, many organizations zealously focus on Health Insurance Portability and Accountability Act (HIPAA) compliance. While a regulatory necessity, HIPAA alone will not account for all the considerations in modern healthcare cybersecurity risk management. In fact, according to Shah, this compliance-centric and healthcare-specific approach can be limiting because of a variety of reasons such as:

*Every technology in a modern healthcare enterprise network is becoming healthcare-neutral.*  
“"There’s really not a whole lot unique about digital health data that justifies complex, expensive, or special cyber security technology,” Shah said.

*Healthcare leaders need to consider the broader computing environment.*  
"Security programs have to keep pace with the evolving threat landscape because hackers do not check your industry. They use tools from everywhere to attack you and that’s what’s important to understand," Shah said. “As an industry, we should look to federal government initiatives like the Department of Homeland Security, NIST, and others as our guidance for approach and tools,”

*Healthcare organizations need to look far beyond healthcare-specific cybersecurity tools and start to adopt security technologies and practices from other industries.*  
"So, whether you are in energy or healthcare or retail or finance, everybody’s got the same problems. And, when we try to say there’s something special about the oil and gas industry, or there’s something special about healthcare, we tend to do ourselves a disservice,” he said. As such, healthcare organizations should mimic best practices and adopt tools that are being used in other industries.
Looking for Help in the Right Places

To more fully protect their organizations, leaders should take cues from security programs of the DHS or the DOD. Leaders need to ask themselves “how do we apply all of this billions of dollars worth of knowledge, effort and expertise … and [apply] it in healthcare so we can benefit. This is one of the first things that leaders should be doing. Don’t just do security on your own and don’t just seek help from other hospitals.”

In addition, leaders should examine what organizations in other industries are doing to protect data. It’s important to learn what energy, food, agriculture and other types of companies are doing because hackers typically are not concerned about what industry they are attacking. In fact, they use the same strategies to attack a wide array of organizations, Shah pointed out.

By adopting this broader perspective, healthcare organizations, for example, are likely to develop comprehensive security programs that go beyond the typical compliance and assessment activities associated with HIPAA-centric initiatives.

“If you just do an assessment once a year, which is basically what HIPAA requires, and you run through an audit once a year or once every other year or a certification, that’s not sufficient,” Shah said. “Please, please, please one thing that you can take away from this webinar is that if all you’re doing is seeing annual controls catalogs and compliance documentation and passing audits, do not think that is real security.”

In fact, Shah pointed out that solely being compliant with HIPAA regulations could result in a false sense of security.

“HIPAA is really more about ensuring that you follow appropriate rules and regulations that are set forth in the law. If you document the right things and step through the right processes, you are likely to be compliant,” Shah said. “But it is absolutely possible to be fully compliant with the law . . . but still leak data in ways that are going to affect patient privacy. So, it is absolutely possible to have compliant insecurity.”

Building Comprehensive Protection

In fact, these compliance-centric initiatives fall short because they typically do not include the all-important risk management, continuous diagnostic and mitigation elements that are a big part of effective security programs.

“Very few organizations are differentiating between point-in-time assessments versus continuous monitoring,” Shah said. Acknowledging the difference is just the start, though. Leaders then need to figure out how to move from merely performing point-in-time status checks to creating an environment of continuous monitoring.
“So, you’ve got to say to yourself, if continuous monitoring is important, how do I do that? At what level?” Shah said. “Only continuous monitoring of each operational asset ensures security.” Beyond complying with HIPAA regulations, healthcare organizations might want to follow the DHS Continuous Diagnostic and Mitigation (CDM) program, which cover 15 continuous diagnostic capabilities. This program directs organizations to ensure that data is secure through the following phases:

| PHASE 1: Endpoint Integrity | • HWAM – Hardware Asset Management  
• SWAM – Software Asset Management  
• CSM – Configuration Settings Management  
• VUL – Vulnerability Management |
| PHASE 2: Least Privilege and Infrastructure Integrity | • TRUST – Access Control Management (Trust in People Granted Access)  
• BEHAVE – Security-Related Behavior Management  
• CRED – Credentials and Authentication Management  
• PRIV – Privileges |
| PHASE 3: Boundary Protection and Event Management for Managing the Security Lifecycle | • Plan for Events  
• Respond to Events  
• Generic Audit/Monitoring  
• Document Requirements, Policy, etc.  
• Quality Management  
• Risk Management  
• Boundary Protection – Network, Physical, Virtual |

https://www.dhs.gov/cdm

In addition, Shah pointed out that the DHS also has created a Continuous Diagnostic & Mitigation Product Catalog (available at: http://www.gsa.gov/portal/getMediaData?mediaId=199735) that lists tools that can be used in a variety of different security areas such as hardware asset management and software asset management. While healthcare organizations are responsible for buying these tools on their own, they don’t have to do all the research into what’s needed. “At least it gives you a good landscape of what is going on as far as a catalog is concerned,” Shah said.
In addition to continuous diagnostics, it is important to utilize a risk management and investment prioritization framework. Shah pointed to a framework from the NIST as a possible model. This framework can serve as a workable model as it:

- Was developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk
- Supports the improvement of cybersecurity for the Nation's Critical Infrastructure using industry-known standards and best practices
- Provides a common language and mechanism for organizations to:
  - describe their current cybersecurity posture
  - describe their target state for cybersecurity
  - identify and prioritize opportunities for improvement within the context of risk management
  - assess progress toward the target state
  - foster communications among internal and external stakeholders

Shah pointed out that using this NIST framework is one option and that healthcare organizations could also use alternative frameworks. However, he emphasized that leaders should understand the difference between a bottom-up risk assessment and a top-down risk cataloging process. With a bottom-up assessment, healthcare organizations will understand their entire computing inventory. With a top-down approach, such as the one offered by NIST, healthcare organizations will “get [their] boundaries in order, understand what’s going on, see what kinds of data that [they] have available and work it from the top-down.”

Finally, Shah emphasized how important it is to get professionals from across the healthcare enterprise involved in data security efforts. As such, information technology professionals cannot solely be responsible for data security and privacy. Health information management (HIM), clinical and other professionals also must become involved to help create a more comprehensive security effort.

“Everybody talks about how important cybersecurity is, and how important data privacy is . . . Nobody really knows how to secure something 100%. Health information management (HIM) professionals know their data. IT professionals know their infrastructure,” Shah said. “So leaving security up to IT, by itself is not a long-term strategy. HIM professionals who want to see their career improved . . . have to understand that security is a complete enterprise problem.”

References
