Health Law Daily

Wolters Kluwer

June 4, 2018

Expert Spotlight—Health care attorney Katie Kenney: Cybersecurity an organization-wide issue, not just IT

By Lisa Yi Hamond

It is imperative that organizations review and invest in their cybersecurity programs to prevent cyberattacks as well as positioning themselves to respond if breaches do occur. According to Katie Kenney, author of Wolters Kluwer's HIPAA: A Guide to Health Care Privacy and Security Law, "It is not a question of 'if' with breach incidents, it's a question of 'when'." Ms. Kenney is a health care attorney at Polsinelli PC. Ms. Kenney regularly advises health care systems, technology/life science companies, vendors, and startup companies on privacy and security issues, including the Health Insurance Portability and Accountability Act (HIPAA), state and federal breach notification laws, 42 C.F.R. Part 2, and the European Union's General Data Protection Regulation (GDPR). She recently spoke to Wolters Kluwer about cybersecurity issues facing hospitals.

Why isn't cybersecurity a priority?

For a number of hospitals, cybersecurity remains a back-burner issue until something bad happens to their organization—meaning, a cyberattack occurs or an unencrypted laptop goes missing. Understandably, hospitals like other businesses must prioritize expenses, but in my experience, the cost of waiting, rather than investing in your cybersecurity program proactively, is night and day.

Why would hospitals be a target for cyberattacks?

Hospitals are susceptible to cyberattacks for a number of reasons, including the fact that they hold a very rich set of data that is valuable on the black market. Underfunded departments are even more susceptible. All too often, we see organizations put off encrypting mobile devices, updating policies and procedures, or conducting an audit to assess their preparedness. Months down the road, we get the call that the hospital has experienced a breach and needs assistance complying with its regulatory obligations, which, for covered entities, includes notifying your patients. It is not a question of "if" with breach incidents, it's a question of when. Taking the time to evaluate and build upon your organization's cybersecurity program prior to an incident occurring, gives your organization the opportunity to mitigate vulnerabilities before they are exposed.

Is it only the information technology (IT) department that needs to be concerned with cybersecurity?

Cybersecurity was (and in many organizations still is) seen as an IT department issue. Today, it is beginning to be seen (and rightfully so in my opinion) as a business issue. Organizations that buy-in and emphasize a culture of compliance are the ones you do not read about in the headlines. Cyberattacks will not slow down. Rather, it is likely that they will only continue to pick up speed; it is imperative that health care organizations catch up.

Do you have any suggestions on how IT can convince upper management about the importance of preventing cyberattacks?

I often see a disconnect between the C-Suite and an organization's IT/Security team. It is important to present the issues facing the health care industry to the C-Suite in a way that will resonate—talk their language, not tech speak. In my practice, I help clients prepare presentations for their Board or C-Suite that focuses on real-life data associated with tangible, publicized breach incidents at similarly situated organizations. Demonstrating to the C-Suite that Hospital X did not encrypt or did not conduct a risk analysis and failure to take these steps resulted in a $5-million settlement with the government, a three-year corrective action plan requiring the organization to pay for an external monitor, legal fees associated with negotiating the settlement, and most importantly, reputational harm, tends to resonate with executives.

Are there any particular scams affecting hospitals?

We are seeing a lot of hospitals fall victim to phishing attacks or experience a ransomware attack. We are also still seeing way too many lost/stolen unencrypted devices containing a wealth of data. Internal threats (careless or negligent employees) are always an issue across the board. In advising clients, I always emphasize the importance of real-life, robust, ongoing training. I recommend conducting simulated phishing attacks to better prepare your workforce for an actual phishing email. The days of click-through HIPAA training are gone. Hospitals need to invest in preparedness. Investment in advanced technology to secure patient data is certainly important, but equally important is investing in training your people.

Do hospitals need to comply with GDPR?

Unfortunately, there is no simple answer—this is a complex question that requires a fact-specific analysis on a case-by-case basis. GDPR applies to (1) US hospitals that are considered to have an "establishment" in the European Union (EU), which does not necessarily mean having an EU corporate entity or physical presence; and (2) hospitals that do not have any physical presence in the EU if they offer goods or services to individuals who reside in the EU. Hospitals should not jump to the conclusion that the GDPR applies just because they have a website that is accessible to EU residents. Additional factors such as whether the hospital includes international telephone numbers on their website for contact purposes or provides options for EU currency conversion, etc., should be examined. GDPR also applies to a US hospital that monitors the behavior of EU data subjects within the EU. For example, GDPR would apply to academic medical centers or hospitals that conduct clinical research monitoring the progress of individuals located in the EU.

Again, the answer to this question is not short and sweet–GDPR's reach is quite broad. If your organization is not sure whether it falls under the GDPR umbrella, we highly recommend taking the time to conduct a thorough review—particularly, now that the effective date has passed.

Is there anything else you would like to share with our readers?

We see some hospitals starting to think of cybersecurity as an organization-wide issue, not just an IT issue. I am hopeful that we will see this trend continue in the future. I do not think cyberattacks will slow down, and unfortunately, I think we will continue to see organizations waiting until a big breach occurs to address cybersecurity. However, I remain optimistic that hospitals will use the many breach incidents that have occurred and the reputational and financial harm that has ensued as motivation to invest in their cybersecurity programs. At the end of the day, I view securing patient data as part of the quality of care you provide to patients. Patients care about their information and ensuring that is secure, to that end, cybersecurity has to move from the back burner to the front (and I think it is, albeit slowly!).