Report on Patient Privacy Volume 18, Number 9. September 30, 2018 With HIPAA in Mind, Intermountain, Others Usher in Age of Virtual Hospitals

By HCCA Staff

Nearly three years ago, Utah-based Intermountain Healthcare launched its first “virtual hospital,” which functions as an advanced form of telehealth for underserved communities. The virtual hospital faces all the same HIPAA privacy and security issues that conventional medical centers and offices face, plus the added challenges that come with managing additional—and constantly changing—processes and vendors for remote electronic connectivity.

In fact, “the development of virtual hospitals and the associated technology stretch HIPAA issues probably to their limit,” says attorney Patricia Shea, a partner with K&L Gates LLP in Harrisburg, Pennsylvania.

HIPAA’s security rule requires that covered entities (CEs) and their business associates, plus all downstream sub-BAs, perform risk assessments to identify threats and vulnerabilities, and to update those risk assessments and revise the management plan whenever there’s been a change to the system, Shea tells *RPP*.

“The biggest pitfall I see is maintaining a current risk assessment and management plan,” Shea says, emphasizing “current.”

Doing so “is a resource-intensive operation,” she says. “To make matters even more critical, OCR [Office for Civil Rights] has repeatedly explained that it views the risk assessment and risk management obligations as extremely important. I advise my clients that this will be, if not the very first thing, at least one of the first things OCR would request during an audit or in response to a ‘bad event.’”

As telehealth becomes more sophisticated and more virtual hospitals open, the risk assessment and management process becomes extremely complicated, Shea says, adding, “the numbers of connections and the people involved grow exponentially. I think this aspect of HIPAA compliance will be challenging for these virtual hospitals because changes happen every day. Changes could be in the form of new functionality, the addition of new sites and personnel, the need for new training. It’s like a spiderweb of connections.”

She adds that “encryption in transit and at rest is a must. This will not eliminate risk, but not doing so in this day and age is likely hard to excuse.”

Consider Vendor Indemnification Clauses

Virtual hospitals also need to consider the nature of their relationships with the CEs they serve, Shea says. “The virtual hospitals should get some concrete assurances from these covered entities as to their compliance with HIPAA’s requirements. These assurances should have some teeth. If their system is going to be accessing or otherwise connecting to the virtual hospital system, you do not want them to be infecting it.”

Shea notes that this would be a factor in the risk assessment and should be addressed appropriately.

A virtual hospital should employ a full-time dedicated information technology staff that’s well-equipped to pinpoint problems quickly, according to Shea.

"As new technology emerges and new risks are identified—e.g., new malware and ransomware attacks—holes are going to need quick attention and patching," she says. "This will be a constant," and "training will also be a constant to address changes and newly identified threats."

Applications used by virtual hospitals must be HIPAA-compliant, of course, but CEs using them "should also get very robust warranties and representations as well as indemnification provisions in their agreements with these vendors. A comprehensive review of the cybersecurity policies would also be recommended," Shea says.

"Compliance is never done," she adds. "You may have a comprehensive risk assessment, management plan, policies and procedures, training and everything else, but you have to constantly re-evaluate them. I think having the operations/professional folks working closely with the technical folks will be crucial in this regard. Moreover, it should happen at each node of the data flow, including the virtual hospitals and the covered entities and business associates they serve."

Intermountain says it pays particular attention to its BA agreements and to its data-sharing agreements, counsels patients on what to expect, and works with employers that want on-site clinics on privacy issues in order to ensure HIPAA compliance.

The health system has 22 hospitals and 1,600 physicians and advanced practice clinicians at about 180 clinics.

In fact, Intermountain Healthcare considers all of its remote services to be part of its "virtual hospital," even though the remote services aren't licensed as a hospital and do not have the primary role for care of inpatients.

"By design, however, we blur the lines, working to best serve our patients by including all our services, when and where they need them," says Dr. Bill Beninati, medical director for Intermountain Connect Care/Pro, the health system's virtual hospital division. "They may be in a clinic, but their primary provider might access telehealth services for higher levels of care."

To Intermountain, telehealth itself as "an extension of what we already do," adds Kyle Finlayson, the system's compliance program manager. "The HIPAA privacy standards we set for our in-person patient visits apply to our virtual ones such as patient identification and ensuring the patient is okay to discuss their care with anyone in the same room or location as the patient."

The health system's standard process for any new project, product or service is to conduct a security review to ensure sensitive and critical data—which includes protected health information (PHI)—are safeguarded during transmission and processing, as well as when it is in storage or at rest, Finlayson says.