COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 2. February 09, 2023 ONC's Tripathi: HIPAA Doesn't Impede Sharing, Requirements Under Info Blocking Regulation

By Theresa Defino

When Micky Tripathi's mom was recently transferred to a rehab facility to recover from a broken hip, the hospital, "right in front of me…printed off her record, handed it to us, and the ambulance driver, for her to bring to the rehab hospital."

After the one-mile trip to the rehab—which Tripathi said is part of a larger health organization with a "very good and well-performing EHR" (electronic health record)—staff took the file and "scanned it into their EHR." Tripathi knew that a network linking the hospital and rehab was "running in the background" of the EHR. Not only is he up on local and regional network development, Tripathi also happens to be director of the HHS Office of the National Coordinator of Health Information Technology (ONC) and is deeply involved in launching a national network called the Trusted Exchange Framework and Common Agreement (TEFCA).[1]

At both the hospital and rehab, "I was looking at them and saying, 'What? You guys are connected. You realize, I know you are connected. This is my job. Why aren't you using that capability?'" The frontline staff seemed just as incredulous, with one replying, "I have no idea what you're talking about…there's an electronic system so we don't have to print this off and scan it? I would love that kind of system!" Tripathi recalled during a recent podcast with the American Hospital Association (AHA).[2]

His experience demonstrated "there's a huge gap between what's implemented by the system itself" and what the chief information officers know about "and what the frontline users know about and have access to and make a part of their day-to-day routine," Tripathi told Nancy Foster, AHA vice president for quality and patient safety policy.

TEFCA is being developed as Congress directed under the 21st Century Cures Act as a technical and governance model "to connect the existing networks with each other," Tripathi said, "so that a hospital user, a doctor, regardless of what network their EHR system" to connect "to every other network in the country in the same way that your cell phone connects to every other cell phone network." ONC anticipates TEFCA, or at least certain early participants, will be "going live" later this year, he said.

In addition to network connectivity, Tripathi discussed how the information blocking regulations his office wrote interact with HIPAA, addressing some of the misconceptions that continue to thwart data sharing. He touched on enforcement, noting that the HHS Office of Inspector General (OIG) still has not issued the relevant rule, and shared how the pandemic accelerated IT adoption and fueled patient engagement.[3]

Tripathi: No 'Tension' With HIPAA

Foster asked Tripathi to discuss the most common questions he receives regarding information blocking rules and to identify common or difficult compliance issues. From her perspective, Foster said she often hears providers' fears that "somehow in complying with information blocking, they'll fall into the trap of violating HIPAA by sharing information with a party who doesn't have a legitimate need to know."

Framing it as a question about whether there is "tension" between information blocking regulations and HIPAA, Tripathi said, "there absolutely isn't. What the information blocking [regulation] says is that information is required to be made available to other authorized parties according to applicable law. So, if HIPAA says that you're not allowed to share information with that other party without patient consent, for example, the information blocking [regulation] absolutely doesn't say, 'Oh, you're required to violate the law and share the information.'"

He added that state laws must be followed. For example, Massachusetts prohibits the sharing of genetic data with parties other than the patient without consent, Tripathi pointed out.

"Just to be clear, this doesn't allow Joe's garage to come pounding on the door of the hospital and say, 'Information blocking. You have to share the information with me.' If applicable law didn't allow it already, then information blocking [rules] doesn't allow it either."

HIPAA and the information blocking regulations are "complementary," Tripathi said. But the difference is that HIPAA regulations are permissive, meaning the information can be shared. Under the information blocking rules, sharing is mandated unless the exceptions are met, he explained. "HIPAA says you're permitted to [share]; information blocking [regulations] say you're obligated to do it," as long as there is not another law forbidding the sharing, Tripathi said.

Confusion Over What Can Be Shared

The most common questions he hears concern the definition of electronic health information and what is required to be shared, Tripathi said. This is "all electronically accessible information," as the law states.

ONC "translated that into something that we thought would be operational" and aligns with "what all hospitals have been required" to share under HIPAA, namely the elements of a designated records set," Tripathi said.

But compliance is complicated by the fact that "a lot of those records in almost any hospital system live outside of the electronic health record," so if a patient requests the entire record, data may have to come from ancillary systems, he said. Hospitals will need to decide "how…to make that electronically available to an authorized user who lives outside of [their] system" and whether any exclusions may be applicable.

As called for in the act, ONC officials have made it clear that "all information needs to be shared unless you have a good reason for not sharing it," Tripathi said. ONC established eight exceptions, which include withholding information as "reasonable and necessary to prevent harm to a patient or another person" or related to a security risk to the provider's system. A number of conditions must be met for each.[4]

Another exception is "infeasibility," which Tripathi explained means, for example, when information is "on a system that literally does not have the ability to send an electronic [item] out of the system."

Missing Enforcement Reg Hurting Compliance?

Lack of a final enforcement rule may be hindering compliance, Tripathi said. While the law established penalties for information blocking by a vendor or health information network, it called for the secretary of HHS "to define those penalties that we'll call appropriate disincentives" without any new authority, Tripathi said. "None of that got defined [during] the previous administration. So, we came in, and now we're working really hard in the department to define" them.

OIG is drafting a final rule, Tripathi noted. He did not suggest when the rule would be published.

The most recent regulatory agenda that tracks government regulations lists March of this year for publication of a final enforcement rule.[5] However, the agenda is a snapshot in time, and dates are often not met, sometimes by months or even years.

While saying that "not that anyone is trying to shirk their responsibilities," Tripathi noted that hospitals have "a lot of open questions" in the absence of a final rule.

Leaders "have to set priorities" and need to know "where does this fit into all my other things," as they are dealing with many other issues, such as the pandemic, hospital capacity, respiratory syncytial virus, etc., he said.

Foster asked Tripathi to identify other "barriers [that] still exist for sending and receiving health data electronically."

He said the "business case" for data sharing hasn't caught on in fee-for-service environments and that there are no incentives for interoperability and data sharing.

"And that's not suggesting that [there's] data hoarding," but providers are doing what they need "to get paid and be able to deal with all the patients in front of [them]," and they aren't "compelled to go out and find all that other information." The provider can "ask the patient" or do "lots of other things that'll get [them] some of that information and then allow [them] to perform effectively under that model."

Conversely, "organizations that have value-based contracts and have moved more into accountable care, all of a sudden [have] a business imperative ... to think about interoperability, think about the sending and receiving of information." In addition to the fee-for-service business model posing challenges, technical and other difficulties—some of which are intrinsic to particular EHRs—get in the way, he said.

Leaders Need to Embrace 'Digital Imperative'

Referring to his experience with carrying his mom's paper chart, Tripathi said the "imperative" and the message for health systems "to move ourselves to digital capabilit[ies] and to think of ourselves as digital natives...hasn't gotten all the way down" in health care systems. This is a "big impediment" to creating the culture change and training required to fully embrace and reap all the benefits of interconnectivity.

The need for training and workflow changes that would be required all the way down the food chain "gets lost in the complexity of hospital operations," Tripathi said.

But he has faith that the younger generation will carry the digital mantle. Using another example from his family, Tripathi said his daughter, a third-year medical resident, quickly became proficient in using EHR systems. In fact, Tripathi joked that she needed to be taught how to use a fax machine.

Hospital leadership needs to recognize the generational shifts and capitalize on them, Tripathi said. Leaders must "start to think more and more as digital natives" and "build that future that [they] want. ONC is doing everything we can to help them do that," he added. "We are always happy to talk to any hospital that has any questions or feels that we could be doing better in helping them on this journey."

Contract Tripathi at micky.tripathi@hhs.gov.

1 Theresa Defino, "Safeguards in New National Network Include Insurance, App Mandates, Cybersecurity Council," *Report on Patient Privacy* 22, no. 2 (February 2022), http://bit.ly/3XX5BZC.
2 American Hospital Association, "Developing a Universal and Secure Electronic Health Information System,

podcast, January 25, 2023, http://bit.ly/3Y1HMzY.
3 Theresa Defino, "Pandemic Accelerated Patient Engagement, Hospital Reporting," *Report on Patient Privacy* 23, no. 2 (February 2023).
4 Office of the National Coordinator for Health Information Technology, "Information Blocking," accessed February 6, 2023, https://www.healthit.gov/topic/information-blocking.
5 Office of Information and Regulatory Affairs, "Amendments to Civil Monetary Penalty Law Regarding Grants, Contracts, and Information Blocking," RIN 0936-AA09, accessed February 6, 2023, http://bit.ly/3jth84b.