Untangling Privacy

Save to myBoK

by **Chris Dimick**

Health IT won't advance far without resolving the complex issue of privacy protections. Can a complicated situation be teased apart thread by thread?

The debate on privacy has become very public.

Privacy advocates, health IT advocates, providers, HIM professionals, federal agencies, and Congressional leaders are speaking out on how to keep health information confidential in an increasingly electronic world.

The issues are so complex and the viewpoints so diverse, in fact, that some healthcare experts believe the healthcare community is in danger of halting any development on the kind of advanced data exchange that could improve care and lower cost.

A possible way out is to stop trying to do too much. Taking on one small aspect of the privacy problem at a time—attempting to tease out individual issues in the tangled debate until they are freed from the ball—could provide a way forward.

Tragedy of the Anticommons

A viable health information exchange requires cooperation among all stakeholders. Without buy-in, the resulting system may be incomplete, unworkable, or unadopted.

Getting that cooperation is easier said than done, according to Darren Lacey, chief information security officer at Johns Hopkins University, based in Baltimore, MD. It is so difficult, in fact, that in Lacey's opinion, it is becoming more unlikely that any nationwide HIE will be achieved due to privacy discussions falling prey to the "tragedy of the anti-commons."

The term, coined by law professor Michael Heller a decade ago in the *Harvard Law Review,* describes what happens when too many people with differing interests and goals own a piece of a project. Each stakeholder focuses on protecting or promoting its own stake, and nothing is achieved, Lacey says.

The issue of privacy in health information exchange is a good example, where differing stakeholders have differing expectations for how—and how much—privacy is provided.

"You are really building the plane by committee," Lacey says, "and then everybody gets veto power, too. That negotiation process will make it very difficult to actually do anything."

When too many egos and issues go into a project, it is unlikely a project will get completed, Lacey says. Such is the case when determining privacy standards. "You will spend all your time trying to negotiate with people," he says.

"Kitchen Sink" Legislation

Privacy issues threaten more than health data exchange. Adoption of electronic health records by physicians and other healthcare organizations may be affected by "kitchen sink" privacy legislation in the US House and Senate, according to Kirk Nahra, Esq., a partner with law firm Wiley Rein LLP, based in Washington, DC. Nahra served as cochair of the American Health Information Community's Confidentiality, Privacy and Security Workgroup.

"Privacy and security issues are creating real impediments right now towards the development of electronic health records," Nahra says. "There is a lot of debate about what the privacy principles should be for use of those records and sharing those records. Right now we don't have any good answers, and the issues have become complicated enough that it is really slowing down progress."

Some pieces of legislation that were designed to encourage the use of electronic health records actually inhibit EHR adoption, Nahra says. A provision in Senate and House bills introduced in late 2008 would create a new set of consent- related obligations that affect only healthcare entities using electronic records. "So only those providers are going to have to get patient consent for a variety of things that they do routinely today without any need for consent," Nahra says. "That says, 'If you adopt this new technology, you now have to do things in a different, harder way.'"

House legislation proposed in late 2008 would also give patients more consent options and wider records access. If passed, this bill would expand privacy rules and could directly affect HIE, Nahra says, since it would allow patients to decide item by item what records can be shared and accessed.

Under the consent bill, patients could tell a healthcare facility when they can or can't use their information for particular purposes. That could mean fragmenting a health record into what is open to share and what is deemed private. That would grind any exchange network to a halt, since each record request would have to be subjected to fine scrutiny by HIM professionals to ensure no privacy laws are breached.

These proposed laws intend to protect patient information, Nahra says, but in reality they inhibit any true protection of information.

"If I say to a hospital, 'You have to get consent from all your patients to do anything you normally do with the information,' there are a couple of choices as to how that would actually happen," he says. "One of them is when you walk in the door as a patient, I say 'Sign the damn thing, and if you don't sign it I can't help you.' That doesn't really help anyone's privacy."

But Nahra isn't sure there is another way. The alternate is for a hospital to say to a patient, "'Here is a list of 500 things we do to run our hospital, check every box.' That is silly also, because if they pick and choose what they are going to sign, that is where it becomes impossible to run the business."

Not only do these options detract from privacy, they also hurt healthcare businesses. That may lead to healthcare officials seeking ways to prevent patients from denying the use of their information, which would end up preventing patients from having a real choice, Nahra notes.

One solution is to abandon omnibus legislation that tries to do everything at once. AHIMA and the American Medical Informatics Association have proposed an alternative approach through the AHIMA/AMIA Joint Advisory Council (AAAC) that would attempt to find solutions to single pieces of the puzzle.

In December AAAC met with members of the Senate Finance and Health Committees and members of the House Ways and Means, Energy and Commerce, and Science and Technology Committees to discuss legislation models that avoid layering on unhelpful privacy rules, says Dan Rode, MBA, FHFMA, AHIMA's vice president of policy and government relations.

Simply adding more individual consent requirements to the HIPAA laws is not the answer, AAAC believes, because additional consents impede the delivery of healthcare while offering no added security benefit. Instead, AAAC recommends standardized authentication requirements and stricter enforcement to better protect health information.

One Piece at a Time

Mark Frisse, MD, MBA, MSc, is a professor of biomedical informatics at Vanderbilt University, and director of regional informatics programs at the Vanderbilt Center for Better Health. He agrees that the way to conquer a complex problem is to handle it piece by piece.

Frisse suggests that healthcare work on solving a piece of the privacy problem from start to finish. Taking a small problem and following through until it is solved often results in solving bigger problems in the process. "How can you win if you try and do everything?" Frisse says.

Such should be the case with privacy standards, he believes. Information exchange developers need to focus on doing one or two smaller steps first, and doing them well, before moving on to another section of privacy regulations.

Keeping it simple is a complex problem when it comes to health information, especially health information exchange. Frisse knows this firsthand as the project director at MidSouth eHealth Alliance, a federally and state-sponsored HIE for greater Memphis, TN. Frisse says his HIE purposefully put simple privacy and exchange principles in place when forming the alliance.

At MidSouth, the group focused on getting data exchanged within one year and doing so with strong auditing and privacy policies in place to appease the participating, competing healthcare organizations. The alliance didn't determine exactly what information should be exchanged; it merely opened it up to each organization and let them decide what to share. There were also no specific data transmission standards set, since officials thought it would bog down the process. The alliance accepts health information in all formats and serves as a translation service between network facilities.

The exchange's development is "incremental over many years, it is not just one big giant leap," Frisse says. "I have just never seen that work. That is crazy."

HISPC: Consensus Achievable?

The Health Information Security and Privacy Collaboration (HISPC) is a collection of state-based work groups first formed to identify the privacy and security barriers to nationwide health information exchange. The work began in 2006 under a contract from the Agency for Healthcare Research and Quality and the Office of the National Coordinator for Health Information Technology. Healthcare professionals, payers, and other HIE stakeholders joined together through HISPC with the hope progress could be made in lowering these barriers.

Critics of the initiative felt the project was too large to accomplish anything substantial. But there were advancements, and in some cases the project showed that large groups of healthcare stakeholders can come together to solve privacy and security problems.

Such was the case in Minnesota, where the state HISPC group took a small piece of the privacy problem—a standardized patient consent form—and followed it through to completion. The form was commissioned by the state legislature, who called upon the HISPC group to assemble outside of the HISPC project and help the state department of health build the document.

The opinions on how the consent form should look were as diverse as the work group's makeup. Providers, insurers, privacy advocates, healthcare lawyers, HIM professionals, and other stakeholders each promoted elements to include in the document. For that to happen, the consent form would have been dozens of pages long—an unacceptable length. Compromise was needed to make any headway, according to LaVonne Wieland, RHIA, CHP, the information privacy director at HealthEast Care System, based in Saint Paul, MN, and member of the Minnesota HISPC group.

There were things on the draft form that just didn't make sense to an HIM professional, Wieland says. "Some of it we were successful in taking off, other parts of it stayed on. But our thought was, Well, it is never going to be [exactly how we want it]. After a while you kind of picked your battles."

The biggest debate came in writing a checklist of the parts of the health record one could request, such as history and physical or discharge summary. Trying to create a single list that made sense for all of the participants was difficult, Wieland says.

After several meetings and lengthy debates, the group whittled down the form to three pages, with the first page containing instructions. A consensus had been met.

Though not everything on the form is how Wieland and other HIM professionals would prefer, she says the overall document is sound.

"Other than just a couple of things, I think everybody was really comfortable with it," she says.

The overall success of the project is hard to measure, Wieland says. On the one hand, the HISPC group found a way to come to a consensus and produce a standardized, state-wide consent form. But since adoption of the form is voluntary, many facilities in Minnesota chose to keep their own individually crafted consent forms—including Wieland's own facility. The group tried to spread the word about the form, but that has produced little results.

After following a small piece of the privacy puzzle and creating a solution, Wieland says she has hope that others can do similar work. But, she acknowledges, there are many people unwilling to compromise and give up ground in the privacy debate. There is a chance that all the problems will be solved, she says, but it will not be easy.

Focus on Today's Problems, Not Tomorrow's

While increasing energy is being devoted to figuring out privacy in electronic systems, Frisse says people should focus on the paper world first before diving into the circuits of the EHR. Absolute consent is an illusion, he says, and consent advocates need to center their efforts on achieving realistic standards rather than trying for ideals. Focusing on today instead of tomorrow will help simplify the privacy debate, Frisse says, and that could help advance development of future data exchange initiatives.

"While I'm sitting in on an undeterminable amount of conference calls by the federal government to understand data-sharing policies, there are very established firms off the grid who make as an exercise knowing everything there is about us," Frisse says.

While HIE stakeholders are trying to solve opt-in and opt-out issues for systems that don't exist yet, he says, consumers have opted in, knowingly or not, to many uses of their information already.

Most privacy advocates are basing their EHR discussions on an ideal world where it's assumed all personal health information is safe today. This is a fantasy, Frisse says, and attention should be focused on the "nitty-gritty of privacy management and paper records" before turning to the EHR.

That is not to say that electronic records can't improve confidentiality. Health IT presents a fresh chance to really protect the privacy and security of health records, Frisse says.

"But it is only a new chance if we go back to the paper-based world and all the nonpaper-based entities and all of the health plan data aggregates and put them under the light of day as well," he says. "We are looking at some possible threatening thunderstorms in the distance, while there is a fire in our house behind our back and we are not feeling the heat yet."

Chris Dimick (chris.dimick@ahima.org) is staff writer at the *Journal of AHIMA* .

Article citation:
Dimick, Chris. "Untangling Privacy" *Journal of AHIMA* 80, no.2 (February 2009): 36-39.