# Privacy in the Spotlight



*by Chris Dimick*

---

*Varying privacy practices that pose barriers to health information exchange are putting HIM concerns in the national spotlight.*

---

The 35-year-old Minnesota woman's winter vacation in the neighboring state of Wisconsin was going great, until her ski snapped and the accident happened. Breaking several bones, suffering internal bleeding, and rendered unconscious, the woman needed immediate and acute medical attention the second she was wheeled into a nearby hospital. What the physicians there didn't know was this woman had a severe allergy to a standard medication.

Hoping to obtain as much medical history on the woman as possible, the Wisconsin doctors put in a request for records to be electronically transferred from her hometown healthcare facility. Time was of the essence. But there was a problem. Minnesota's state laws require authorization, or patient consent, in order to disclose any medical information, even for treatment purposes.

Without time to wait on the records, physicians unknowingly administered the medication the woman was allergic to. This caused a severe adverse reaction, heart failure, and eventually death. Had a fully functional health information exchange network been in place—one with both the technology and the aligned policies for sharing information—the woman likely would have been saved.

### The Key Issues

The HISPC report summarizes the privacy and security barriers to HIE under the following categories:

- Variations in interpretation and application of consent
- Misunderstanding and differing applications of the HIPAA privacy rule (including minimum necessary, redisclosure, professional judgment, and accounting of disclosures)
- Misunderstanding and differing application of the HIPAA security rule
- Insufficient or varying security practices (including authentication and authorization, screening controls, audit programs, transmission, and security infrastructure)
- Lack of consumer trust in an organization's ability to protect information and lack of one organization's trust in another's ability to protect information
- Missing and outdated state laws (including general misunderstanding of the intersection of state law with federal rules)
- Networking issues, including concerns over the ability to develop and operate a network such as legal, governance, technical, and financial issues
- Lack of a "standard, reliable" method of matching patients and records, which could lead to inappropriate disclosure of personal health information
- Interstate issues, which encompass unaligned state laws on issues such as specially protected information and minor's rights
- Variation in practices related to disclosure of personal health information
- Cultural and business issues, such as conservative approaches to data exchange, resistance to change, variation in definitions of privacy terms, and control of data

## The Problem with Variance

This story is fictional, but it illustrates the complications healthcare providers face when trying to exchange medical information across state lines. The variance in authorization and consent laws among the states is just one of several issues identified as barriers to developing interoperable health information exchange networks in research published this summer by the Agency for Healthcare Research and Quality (AHRQ).

"Privacy and Security Solutions for Interoperable Health Information Exchange" summarizes the findings and recommendations of 34 state-level work groups that form the Health Information Security and Privacy Collaboration (HISPC). The work groups, representing 33 states and Puerto Rico, gathered stakeholders throughout the healthcare community to identify the privacy and security issues that hamper the exchange of health information.

The project was conducted by Research Triangle Institute International on a $17 million federal contract to "better understand what policies and practices need to be in place within and across states to both protect health information and promote nationwide electronic health information exchange," the report states.

Privacy and security issues are just pieces of the greater HIE puzzle. Other issues exist, such as the technical aspects of developing, standardizing, and implementing the IT systems that enable interoperable data exchange. The industry also is struggling to find sustainable governance and funding models for exchange networks.

But the HISPC work turns attention to privacy policies, which have not received the same focus to date. Many of the issues identified in the report will be of no surprise to HIM professionals, who have wrestled with these concerns for years. But the research has the potential to shine a national spotlight on the pressing need to address them.

### A "Complex Patchwork"

Individual US states lack consistency in how they approach the privacy and security of health data. This variance is a major barrier to not only developing a nationwide, interoperable HIE network, but also to merely transferring health data from one organization to another.

When HIPAA was introduced, it was intended to establish a minimum set of privacy safeguards. Some states and organizations enacted privacy and security practices and laws that provide protections above and beyond the federal law.

Adding to the complexity are differing practices at the organization level. This makes the exchange of information within a state difficult. Programs like Medicare and Medicaid also have their own privacy policies and procedures, further diversifying privacy practices. A healthcare provider hoping to obtain a patient record from another organization has to keep in mind federal, state, facility, and program laws and policies.

"That is the single most significant issue, in my view of this project," says Walter Suarez, MD, MPH, president and CEO at the Institute for HIT/HIPAA Education and Research. Suarez co-authored the national AHRQ report. "This [variance] creates a very complex patchwork of factors and elements that affect how [organizations] do health information exchange, or how much of it [they] can do."

## No Consensus on Consent

Such variance is clearly demonstrated in how states and organizations handle consent for release of information. Consent issues are a major barrier to health information exchange because the industry lacks standardized mechanisms for when patient permission is needed to release health information. HIPAA states that consent is not required for record exchange if protected health information will be used for treatment, payment, or healthcare operations.

But since HIPAA serves as a floor for privacy protection, not a ceiling, several states have enacted laws that require consent be obtained for all uses before patient information can be released to an outside party. Organizations have even enacted similar business policies, according to the report, to reduce the risk of "liability for wrongful disclosure."

Before a regional or nationwide HIE system could be built, these differences in consent requirements would need to be simplified, the report notes. "In Wisconsin, for treatment purposes, we don't have to have an authorization, an informed consent," says Chrisann Lemery, MS, RHIA, a compliance specialist with WEA Trust Insurance Company in Madison, WI.

Lemery served on the Wisconsin HISPC work group. "Some states require an authorization or consent in order to share information for all reasons. So that puts the barrier up."

Many of the 34 work groups noted confusion about the HIPAA privacy rule requirements on consent. They reported a general misconception that patient permission is required to disclose information for treatment.

Margie White has seen this first hand at Columbus Colony Elderly Care, a facility for the deaf that attracts residents from around the country. White, MS, NHA, RHIA, CPHQ, is an assistant administrator with Columbus Colony Elderly Care in Westerville, OH, and serves on the Ohio HISPC work group. When an out-of-state resident comes to her facility, gaining a full medical record on the person can become difficult due to differing state and organization privacy laws. This is true especially when trying to obtain behavioral health information, she says.

There isn't even a standard consent form that states can use. When HIPAA was changed to remove the requirement that consent was needed in order to exchange information for treatment purposes, it also removed any format for a consent form, which further adds to the variance, says Joy Pritts, JD, a research associate professor at the Health Policy Institute at Georgetown University and a co-author of the AHRQ report.

Many of the state groups recommended creation of common approaches to consent. They also identified the need for standard definitions of privacy terms. Use of the words "authorization," "release," and "consent" differ between states and organizations. HIPAA uses the term "authorization" in a way that most state laws do not, Pritts says.

# Blaming HIPAA

Nearly five years after its implementation, many people in healthcare are confused about privacy rule requirements, the report states. In fact, the work groups noted that HIPAA has become a kind of catchall phrase to describe why certain privacy and security rules are in place—even when HIPAA doesn't actually specify the practice.

## HIM's Role

HIM professionals had direct involvement in the HISPC project. The involvement is a natural one, because privacy, security, and data exchange are intertwined in an HIM professional's role as a steward of health information.

Any future formation of an HIE network will surely change how HIM professionals organize and release health information. For this reason, more HIM professionals should get involved in this debate at the local level, says White. "Privacy and security are what we are about. It is important those issues are solved and that we are at the table as this is happening," she says.

HIM's input is essential, agrees Lemery. HIM professionals "live and breathe" privacy and security every day, she says, which was evident during her group's discussions. Team members from outside HIM often commented on all the things they learned from HIM members, Lemery says.

Lemery expects that once a fully operating nationwide HIE is in place, HIM will have limited contact with the actual data exchanges, which would be largely automated. But first developing and then auditing the exchange process are tasks that call for HIM involvement.

This will not be an easy task. Susan Manning, RHIA, is an independent healthcare consultant who served on the Wisconsin HISPC group. "The toughest thing is finding the balance between patient rights and what information providers need to know to provide patient care," she says.

"One of the major issues identified was the continuing widespread confusion about the HIPAA privacy rule," Pritts says. "HIPAA has become the poster child for why health information will not be released—whether or not it is the source for that restriction."

Suarez notes that this "blaming HIPAA" approach usually does not originate in an organization's policies; it typically results with the front-line employees who execute the policy. The state groups report inconsistency in how employees are

implementing organizational policies. The restriction of data exchange without prior consent could be due to state law or could be due to the organization's own policies, but many will cite HIPAA as the reason.

"These are complex issues and explaining all this together is difficult," Suarez says. "You need 10 lawyers and charts and a courtroom to discuss this, and the poor receptionist who is taking the actual consent forms—the first person that addresses the patient—is the one who has to deal with this."

The problem highlights a critical need for education about HIPAA, Pritts says. "One of the lessons here is how much education is needed when a new federal standard is implemented," she says.

### Variability in Security Practices Raises Similar Barriers

While this article focuses on the many privacy issues raised in the HISPC work, the state teams also discussed a variety of issues revolving around security. The two topics cannot be separated in practice, of course (since privacy relies on security).

The work groups identified possible barriers around four major security issues, sometimes referred to as the four As: authentication, authorization, access controls, and audits. As with privacy barriers, a lack of consensus and standards poses the greatest challenges.

"That immediately is a major factor limiting the ability for health information exchange," Suarez says. "Because if I am exchanging data with someone else and we don't use the same authentication, authorization, access controls, and audits, then we are going to have some problems."

For example, organizations currently authenticate record requestors in different ways. If they attempt to do so as part of a nationwide exchange system, the system would become overburdened with myriad authentication protocols, log-ins, and passwords.

## Arch Conservatives

Lemery agrees that more education is needed on privacy and security procedures nationwide. When people don't fully understand a requirement and are fearful of doing something wrong, they act conservatively. That can serve as a barrier to legitimate data exchange.

"Entities expressed—and this was something documented in the report—that they have seen cases when providers do not send clinical information to other providers because of concerns, fears, and conservative interpretations of regulations," Suarez says.

Organizations are concerned about their liability for accidental and inappropriate disclosure of health information, which the report says causes them to implement privacy and security policies that are more conservative.

When unsure about state and federal privacy laws, organizations will default to not disclosing information out of a fear of litigation as well as fear of damaging their reputations, Pritts says. "Nobody wants to be above the fold in the *New York Times,*" she says.

Being concerned with security and privacy is not a bad thing, of course. Organizations just need to figure out a balance so that legitimate providers get the information they need to help patients, Pritts says.

## Mistrust in Others

Work groups also noted the role of trust; one identified it as the single most significant issue it documented. Some organizations are hesitant to share information if they are unsure of the other entity's privacy and security practices. They fear that if the other entity mishandles the patient information, they might also be held accountable for sharing the information in the first place.

Organizations thus evaluate the risk of exchanging information. “This causes discrepancies when you are trying to exchange between the organization that is to the letter of the law and the one who is willing to take risks,” Lemery says.

## No Closure on Redisclosure

A lack of standards for redisclosure of information is also hindering HIE. HIM professionals are familiar with the following example.

Provider A recommends patient Mrs. Smith to Provider B and transfers Smith’s medical record. Provider B treats Smith and adds Provider A’s record to their copy of Smith’s record. Now Provider B refers Smith to Provider C. Can Provider B share Smith’s entire record with Provider C, including the information that originally came from Provider A?

HIPAA says that is fine, since the information is being exchanged for the sake of providing treatment. But what if Mrs. Smith had prohibited Provider A from releasing certain pieces of her record? Provider A would be held liable for sharing that information with Provider B. But could Provider B, having no prior knowledge of a confidentiality agreement, be held liable for disclosing the restricted information to Provider C?

This issue has yet to be determined, and some state work groups identified it as an issue that must be resolved for HIE to move forward.

## Special Treatment for Special Data

Though HIPAA allows patient data to be exchanged for treatment purposes without consent, other federal and state laws enact additions to that rule regarding “specially protected information.” Under these laws HIV status, mental health records, substance abuse information, and similar sensitive information can only be released if consent is first received from the patient.

This complexity requires any electronic system in an HIE network to distinguish when authorization is needed for discrete pieces of a record. The system also will need to assess the information being requested and who is requesting it, Lemery says.

“You will have to have a process in place to segregate that information,” she says, “then also have a process in place to get authorization before you can exchange it between entities. This requires extra steps, and there are few vendors that [currently] can separate the information.”

## Missing and Outdated State Laws

Some HISPC groups found that their states laws weren’t ready for HIE. Some groups had problems finding the privacy and security laws in their state code. Others noted concerns that the law was too antiquated to apply to electronic HIE. “Some laws don’t even address an electronic process,” Lemery says. “It causes confusion because of the way the law is written. It is pretty obvious that it is only considering paper.”

Eleven state groups mentioned a lack of state laws that could be applied to HIE. “This just convolutes the issue because, well, if the law is silent, what does that mean we should do?” Lemery says. Ten groups identified the generally confusing conditions of state laws as a critical issue, and 11 reported the use of overly conservative business practices because of confusion or lack of knowledge about state privacy laws.

That’s not entirely bad news. The lack of formality may be a good thing for future HIE. “The perception that most state laws need reform may present an opportunity to develop uniform, or at least consistent, HIE-related state laws,” the report notes. The effort would require collaboration to ensure standardization among the states.

## Shining a National Spotlight, Creating a State-level Dialogue

The success of the HISPC report lays not just in the identification of national problems. Assembling the 34 work groups to discuss these barriers was a large effort in itself and a great step forward, Pritts says. “I think what the project did very well

was it got the states talking both within the state and across state boundaries about some of the issues that they need to address," she notes.

The privacy and security barriers identified in the report were not the most important element of HISPC's work. The fact that the project created the infrastructure to move privacy and security issues forward in 33 states and one territory is the "single most significant value and investment," Suarez says. "Overall, the report showed that progress is being made toward interoperability," he says.

The report may not offer breaking news to HIM professionals, but it does move HIM issues into a national spotlight. "It has been talked about with those of us who live and breathe exchange, disclosure, release," Lemery says, "but does anybody else really understand that? They may have thought they understood it, but now you have a report that tells you all the [privacy and security] issues there and all the variations that exist."

The published report is not the end of the HISPC project. The individual state work groups have drawn up plans to implement solutions to specific privacy and security issues. They will work on these localized solutions through the end of the year.

A second round of meetings began in September. In this phase, state groups join to form multistate collaboratives. These collaboratives are made up of state groups that took part in phase 1 of the project and new groups from states that did not participate initially. In these collaboratives, the groups will discuss regional and national solutions to privacy and security issues, expanding the reach of the original work. "That is very exciting," Pritts says.

## Full Reports Online

To read "Privacy and Security Solutions for Interoperable Health Information Exchange" visit http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_661882_0_0_18/AVAS.pdf.

Related HISPC reports and further information on the project are available at the AHRQ and RTI Web sites at http://healthit.ahrq.gov and www.rti.org.

Suarez agrees. As a self-described HIPAA evangelist, Suarez says he couldn't be happier with the project. "With my 20 years of experience in this field, this project was by far the single most significant effort done on this issue," he says. "This is an unprecedented, landmark study, a unique opportunity to move and advance and help create this local infrastructure."

The project is a step toward developing a national framework for HIE, according to Pritts. "I am convinced that we can develop a nationwide health information network that preserves privacy," she says. "It can be done, if we are willing to do it."

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

**Article citation**:
Dimick, Chris. "Privacy in the Spotlight" *Journal of AHIMA* 78, no.10 (November 2007): 28-33.