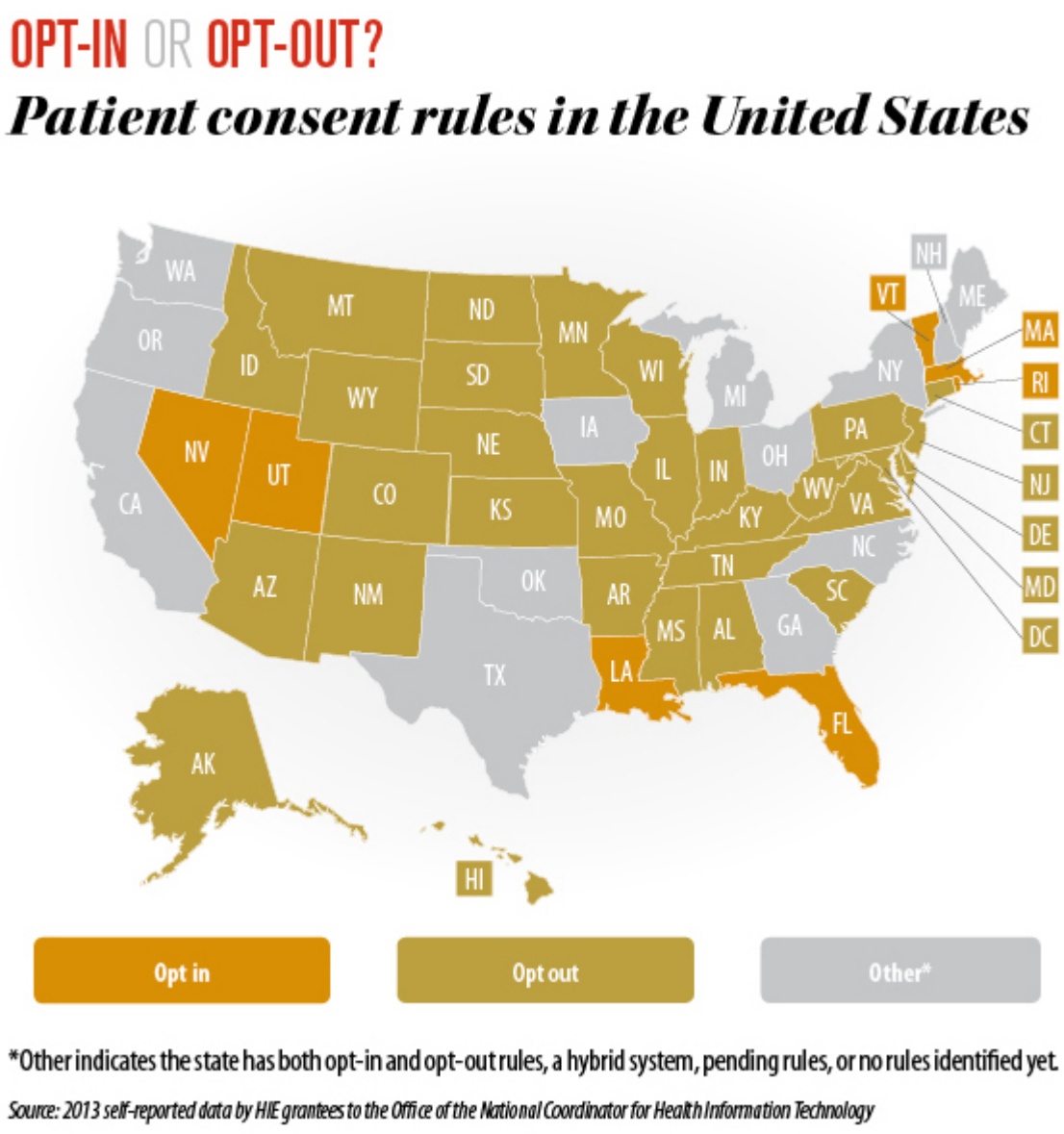
Health information exchanges introduce patient consent questions

Experts offer advice on technical, legal and ethical implications

Publish date: JUL 08, 2014

By: Ken Terry



As physicians, hospitals and health systems increasingly share patient data between providers and across healthcare organizations, the issue of patient consent becomes critical. Should patients be required to opt in or opt out of health information exchanges (HIEs)? And what are physicians' legal obligations in making sure this data is exchanged securely and accurately?

Although meaningful use stage 2 has been effectively delayed, physicians who wish to attest to it this year or next will have to exchange patient information electronically at transitions of care, including referrals. Physicians might also be asked to send records online to other doctors when patients self-refer to them.

Depending on how this information is exchanged and what is exchanged, patient privacy issues may come into play. Physicians need to be aware of state and federal legal requirements and should follow best practices to ensure patient privacy and avoid liability. This includes understanding the role of patient consent in the exchange process.

In general, the federal Health Insurance Portability and Accountability Act (HIPAA) rules allow treating providers to exchange information about patients they have in common, regardless of whether they are part of the same organization. Patients are already asked to sign HIPAA privacy notices and consent forms that allow their information to be disclosed to designated individuals. Depending on the state, patients may also have to give specific consent for information to be exchanged through HIEs that transfer electronic data between participating providers or provide access to it online.

Nearly half of the states have or plan to have these "opt in" requirements for health information exchange in their statewide HIEs, according to the Office of the National Coordinator of Health IT (ONC). Most of the other states have "opt out" policies that allow patients to choose not to have their information exchanged online.

The different ways states treat electronic data exchange could have implications for the viability of HIEs and for physicians' ability to access information on their patients from other providers. "Opt in makes it hard to operationalize the full benefits of HIEs," says David Harlow, a healthcare attorney based in Newton, Massachusetts and author of the HealthBlawg blog. "With an opt in requirement, a lot of people don't bother to opt in."

That is not necessarily the case, however, if people are educated about their choices. The Massachusetts eHealth Collaborative (MAeHC), for example, built HIEs in three communities and incorporated an opt in policy. Front-desk staff in doctors' offices gave patients brochures about the HIEs and asked them to sign consent forms. More than 90% did, Micky Tripathi, chief executive officer of MAeHC, told iHealthBeat.

Another issue is how consent requirements in different states affect the ability to exchange records across state lines. Northern "snowbirds" who winter in the South, for example, may need to have health information exchanged between their home states and the states where they reside in the winter. If some states allow information exchange unless patients opt out and others require them to opt in, "that hamstrings the provider in the other state," Harlow says.

That only begins to describe the impact of variations in state laws. For example, Indiana privacy laws are no more restrictive than HIPAA, notes Eric Thieme, chief administrative officer and general counsel for

the Indiana Health Information Exchange (IHIE), one of the nation's largest and oldest HIEs. IHIE has an opt out policy to that health system participants adhere to, he says.

In California and New York, however, providers can't agree on what the state privacy laws mean in regard to HIEs, Thieme says. A New York law says a patient doesn't have to give consent for data to go to an HIE, but must consent for anyone to view the data in the HIE. That muddies the waters, he notes.

To date, the federal government has not tried to impose a national standard in this area. An Office of the National Coordinator for Health IT security and privacy framework for state health information exchanges advocates what it calls "meaningful consent"—i.e., consent that follows substantial patient education—but does not take a position on opt in versus opt out.

Physicians may wonder how to remember which patients opted in or out when they transmit data to an HIE. An electronic health record (EHR) check box may show the information, but that doesn't necessarily prevent practices from making that patient's data available to an HIE along with all of their other patient records.

The Indiana exchange has developed a simple solution: Its members send EHR data on all of their patients, along with a list of those who have opted out. IHIE uses a software mechanism to block other HIE participants from viewing information on those patients, Thieme says.

The sensitive data quagmire

Federal and state laws require that certain kinds of data be segregated before records are exchanged between providers. This includes psychotherapy notes and alcohol and substance abuse treatment records.

IHIE prohibits participating providers from sending records of either type. Beth Israel Deaconess Medical Center (BIDMC), a Boston-area healthcare system, "locks up" won't make patients' mental health records available even to other providers in its own system without patient consent, BIDMC chief information officer John Halamka told InformationWeek Healthcare.

While laws and policies in this area are fairly straightforward, the picture becomes murkier where other types of sensitive data are concerned. For example, patients may not want other treating providers to see that they have been diagnosed with HIV or another sexually transmitted disease. Thieme says those are the most frequently requested exclusions in Indiana, but some patients may not want to disclose information on other health conditions either.

Even if providers want to accommodate these patient requests, today's EHRs make it difficult for healthcare organizations to do so. Experts say that EHRs have difficulty segregating sensitive information, partly because much of the data is embedded in free text, rather than structured fields that can be manipulated.

Beyond these categories, providers are not legally required to withhold certain data in patient records when they exchange them with other treating providers. "Under HIPAA, the patient has the right to segregate some things only if the provider is willing to do it," says Harlow. "Most providers are not willing to customize anything, because they don't have the tools to do it easily and reliably. So they're just going to say no, except for some things that must be segregated and not go to a payer if the patient so desires."

Partly because of the difficulty of sequestering specific information, Mary Griskewicz, senior director of health information systems for the Health Information Management Systems Society, says it's simpler from a legal standpoint to ask the patient to allow having all of his or her records exchanged.

"From a risk assessment perspective, that's the way to go," she says. "A lot of providers say, basically, that if you want to get treated, you have to agree."

Liability issues

In general, healthcare organizations are not liable for security or privacy breaches at other organizations with which they've exchanged patient data, Harlow says.

"If the handing off of the data can be documented to have

5 QUESTIONS TO ASK AN HIE

1. What state regulations do you have to comply with?
2. How do you make sure that only patients who have opted in (or in an opt out state, those who have not opted out) can have their records viewed by other providers?
3. Are you willing to sign a business associate agreement that specifies your security duties under HIPAA?
4. Can you segregate certain kinds of data when that is requested by a provider on behalf of one of their patients?
5. Will you provide an audit trail for an individual patient if their provider requests it?

taken place in an appropriate manner, the next entity would have primary liability for any such release," he says.

Under the HIPAA Omnibus rule released last year, the sending provider could potentially be held liable for a breach unless the provider vetted the security systems and policies of the receiving provider, but that's only a legal theory at this point, he adds.

What's not theoretical is that the HIPAA rule treats business associates of providers as subcontractors who share liability for security breaches of patient data. So healthcare providers have demanded that these non-HIPAA-covered entities sign business associate agreements (BAAs) that specify their responsibilities.

Harlow doesn't think that HIEs must have such agreements if all they do is act as "pipes" to transmit data from one provider to another. But if they touch the data in any way—as many HIEs do when they help providers analyze data—they must have a BAA, Harlow says. IHIE has BAAs with all of its customers and vendors who handle its personal health information, Thieme notes.

According to Harlow, the HIPAA rule has yet to be finalized in the area of providing patients access to "audit trail data" showing who viewed their data and when. IHIE will provide this data to organizations that request it for patients. So far the exchange has received few such requests, Thieme says.

Common sense patient consent

Ultimately, health information exchange is about enabling physicians to see the information they need to provide the best possible care to their patients, Griskewicz says. In certain situations, the physician must make critical decisions about whether to obtain that data or supply data that a colleague needs to treat the patient.

"If you enter into a relationship with a provider, you do that because you want their first duty to be to treat you," she says. "If the doctor is treating a person that has a condition and can't represent themselves, the doctor will do what they have to do."

"There has to be a level of faith and trust. If you have a particular condition that you don't want shared, providers are going to look at their policies and procedures and see what they can accommodate."

Patient consent issues in health information exchange have not yet been fully worked out, and physicians should be aware of that, even as they try their best to comply with laws and policies. As the electronic interchange spreads, public awareness will increase, "and the differences between opt-in and opt-out may get messy," Harlow says.

But over time, he adds, consumers will appreciate the improvements in healthcare that will result from the increased flow of information. "In the long run, it will be a good thing, and it could reduce the duplication of diagnostics and get the right care to patients sooner."

http://medicaleconomics.modernmedicine.com/medical-economics/news/health-information-exchanges-introduce-patient-consent-questions