Enabling HIE While Protecting Privacy: An Overview of State Legislative Approaches

Save to myBoK

by **Kory Mertz**

States view health IT as a key component of their efforts to improve healthcare, and in recent years they have made significant efforts to address the challenges to its implementation. From 2007 to 2008, state legislatures introduced more than 380 bills with provisions relating to health IT. Of these, 140 bills passed in 44 states and the District of Columbia—almost a fourfold increase compared to 2005–2006.[1,2]

State legislative health IT efforts focus on five areas: planning, targeted financing initiatives, updating privacy laws to facilitate health information exchange (HIE), promoting HIE, and advancing adoption and use. This article analyzes initiatives to update privacy laws.

Privacy Concerns Inhibit HIE

Patient and provider concerns about privacy and security are inhibiting HIE in many states. Patients fear that sensitive health information related to dire or stigmatized diseases will be disclosed and used against them in decisions regarding health insurance coverage or employment. Providers concerned about varying interpretations of state and federal privacy laws and the liability for violations are often reluctant to exchange data.

States can fine-tune their health privacy laws to help alleviate these concerns and build consumer confidence in the integrity and utility of HIE systems.

State Approaches

State lawmakers are taking differing paths as they attempt to capture the benefits of mobile health data while addressing patient and other healthcare stakeholder concerns. The items spelled out below are the building blocks of state legislative efforts to address privacy while enabling HIE.

Definition of key terms. In light of the myriad health IT terms swirling around the healthcare industry today, states are clarifying the definition of common terms in their health IT legislation. Terms and their definitions vary across states, but they can include health IT, electronic health records or electronic medical records, and HIE. The structure of data exchange in the state also influences what terms are defined. For instance, states using a record locator or regional health information organization must define these terms.[3]

Privacy. As healthcare enters the digital age, some states are modifying their consent policies. In doing so, they are balancing patient desire to control where data flows with provider concerns about having access to all relevant information for treatment. Another concern is the cost of implementation.

States face a number of key policy decisions as they look at patient consent. Under what circumstances should consent be required? How should consent be structured (opt-in, opt-out)? Will additional levels of granularity be allowed, or will patients have to choose between including all their information for exchange or none?

States are taking different approaches to these policy decisions. Minnesota (opt-out with granularity), Rhode Island (opt-in with granularity), and Nevada (opt-out) provide three contrasting approaches.

In Minnesota, patients have the right to opt out of the patient index in total, or they may restrict which providers have access to their information. Consent is required in nonemergency situations. Patients in Rhode Island must opt in to the HIE. They can

control which providers may access their data, but their authorization is not required for some public health, emergency, and administrative uses. See "Comparison of Privacy Provisions in Minnesota and Rhode Island" [below].

Nevada's statute specifies that HIPAA shall preempt any more stringent state laws related to the electronic exchange of health information by covered entities. The bill allows patients to opt out of data exchange, with an exception for Medicaid and SCHIP patients and when required by HIPAA or state law.

Security. States are incorporating security requirements standards in their laws. Examples include requiring audit logs, creating standards for who can access data in an HIE, and how users will be authenticated.

Universal consent or authorization form. To address differing interpretations and applications of federal and state privacy laws, some states have established a common consent or authorization form and require providers to accept it.[4] For example, the Oklahoma legislature ordered the state board of health to create a standard authorization form through the Health Information Privacy and Security Collaboration for the exchange of health information. Providers who use the form and follow the board's instructions are immune from liability under state privacy laws that may arise from the exchange of health information. Use of the form is not required.

Access to data in an emergency. Some states are outlining a process that gives providers the ability to access a patient's data from an HIE in an emergency if the patient cannot provide consent.[5] See "Comparison of Privacy Provisions in Minnesota and Rhode Island" for examples of how Minnesota and Rhode Island addressed this issue.

Provider liability. Providers are concerned about liability if they treat a patient based on incorrect or missing data obtained from an HIE. Some states have enacted laws that include provisions giving providers immunity if they rely in good faith on information provided through the HIE in the treatment of a patient.

Outdated provisions. Outdated statutes may hinder the exchange of data, and states are updating their health IT laws to remove these barriers. A simple example of this comes from the prescribing process. Many laws enacted prior to the digital era required that prescriptions have a wet signature. This requirement prohibited electronic prescribing, and states with these policies had to update them to allow electronic signatures.

Enforcement mechanism. Providers must be held responsible for any noncompliance with health IT legislation. Some states have created a credible mechanism for enforcing standards and penalizing certain violations. See "Comparison of Privacy Provisions in Minnesota and Rhode Island" for examples of the penalties Rhode Island and Minnesota established.

States that want to advance HIE generally either enact comprehensive legislation or modify existing statutes. Comprehensive legislation addresses the broad range of issues in HIE. On the other hand, states that modify existing statutes generally update existing statutes to eliminate provisions that limit or thwart HIE.

In recent years, state policy makers have put into place a variety of approaches to address privacy concerns while enabling HIE. Healthcare stakeholders, states, and the federal government have much to learn from the leading states. In the coming years, states will continue to move forward on health IT as they seek to improve healthcare quality and reduce costs.

Comparison of Privacy Provisions in Minnesota and Rhode Island

State lawmakers are taking varying approaches as they attempt to balance the benefits of HIE with the need for strong privacy protections. This side-by-side comparison of privacy provisions in Minnesota and Rhode Island demonstrates how each state is dealing with consent and emergency access, provider liability, and penalties for violations.

	Minnesota Minnesota Health Records Act	**Rhode Island** Rhode Island Health Information Exchange Act of 2008
Summary	Allows creation of record locator services (RLS). An RLS is an electronic index of patient identifying	Establishes a statewide HIE under state authority.

	information that directs providers to the location of patient health records held by providers and group purchasers.	
Consent and access to data in an emergency	An RLS can be created without patient consent. Patients have the right to opt out of the RLS in total or can exclude specific provider contacts from the system. Consent is required to search an RLS for the location of a patient's records except in an emergency. To facilitate the real-time exchange of data, one provider can electronically represent patient consent to another. To do so, a provider must have a signed and dated patient consent form authorizing the release. In addition, the provider releasing the record shall document: • the provider requesting the health records; • the identity of the patient; • the health records requested; and • the date the health records were requested.	Patients must opt in for their data to be included in the HIE. Patients who choose to opt in can decide which providers will have access to their data. If a patient opts in, his or her authorization is not required for release to: • public health authorities for specified functions; • healthcare providers for diagnosis or treatment in an emergency; and • the RHIO for operation and administrative oversight of the HIE.
Provider liability	When requesting health records using consent, or a representation of holding a consent, a provider warrants that the request: • contains no information known to the provider to be false; • accurately states the patient's desire to have health records disclosed or that there is specific authorization in law; and • does not exceed any limits imposed by the patient in the consent.	Provides immunity to healthcare providers who rely in good faith upon information supplied by the HIE in the treatment of a patient.
Penalties	An RLS that negligently or intentionally violates certain provisions is liable to a patient for compensatory damages plus cost and reasonable attorney fees. Anyone who inappropriately discloses a patient's data is liable for compensatory damages caused by an unauthorized release, plus costs and reasonable attorney fees. Providers who violate the statute can face disciplinary action by the appropriate licensing board or agency.	The bill establishes civil and criminal penalties for violations of the statute. Attorney fees may be awarded by the court to the successful party in any action under this chapter.

Notes

1. National Conference of State Legislatures. “Health Information Technology Legislative Tracking Database.” Available online at www.ncsl.org/programs/health/forum/Hitch/HIT_database.cfm.
2. eHealth Initiative. Third Annual Survey of Health Information Exchange Activities at the State, Regional, and Local Levels. Washington, DC; eHealth Initiative, 2006.
3. Ruth, Julie, Christina Stephan, and Patricia Gray. “Harmonizing State Privacy Laws for HIE.” Presentation at the Health Information Security and Privacy Collaboration National Conference, Washington, DC, March 2009.
4. Ibid.
5. Ibid.

Kory Mertz (kory.mertz@ncsl.org) is a policy associate for the National Conference of State Legislatures in Washington, DC.

Article citation:
Mertz, Kory. "Enabling HIE While Protecting Privacy: An Overview of State Legislative Approaches" *Journal of AHIMA* 80, no.6 (June 2009): 50-51;57.