

# Breaking Down Privacy and Security Barriers to HIE

Save to myBoK

by Harry Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA

As noted in the article “Confusion Continues over HIPAA Minimum Necessary Standards,” (*J AHIMA*, Nov-Dec 2007) the state-level research under the HISPC project identified a number of privacy and security barriers to health information exchange (HIE). Several reports came from this project, released by the Agency for Healthcare Research and Quality.

The report “Privacy and Security Solutions for Interoperable Health Information Exchange” recommends actions the healthcare industry can take to get past these barriers. This article outlines some of the report’s 13 recommendations.

## Improve Communication

One gap identified by the project was a general lack of stakeholder and state project team knowledge regarding HIE and health IT initiatives currently under way. In spite of this global knowledge gap, a number of states were undertaking cutting-edge HIE initiatives. State-level health IT and HIE activities that do not align with federal privacy and security initiatives create more variation.

To deal with the existing knowledge gap the report recommends that action be taken to facilitate communication and collaboration between state and national privacy and security efforts. The healthcare industry should set a clear direction through consistent, regular, formal, and accurate communication.

The report proposes three recommendations to coordinate regular formal communication:

- The formation of a confidentiality, privacy, and security work group, chartered to serve under the direction of the successor to the American Health Information Community (AHIC). In order to ensure communication, one member from the work group would serve as a state liaison to leaders of the state-level privacy and security bodies.
- Under AHIC leadership regional meetings should be hosted at least twice a year in different regions of the country. State and local privacy and security leaders would be invited to attend and have the opportunity to inform the AHIC successor of activities and needs at the state and regional levels.
- To advance the national vision, the Department of Health and Human Services (HHS) should oversee the publication of a monthly or bimonthly electronic privacy and security newsletter charged with highlighting the progress of the various privacy and security initiatives under way at the state and local levels.

## Develop a Governance Model

Currently no universally accepted electronic HIE governance model or widely recognized set of governance functions exists. State contract stakeholders have often cited the need for a formal state or local coordinating body as a means to organize and monitor electronic health information exchange. The proposed HIE coordinating body could provide the infrastructure and processes needed to develop, promote, implement, and enforce electronic HIE policies, procedures, and practices.

The report proposes forming such a coordinating body and charging it with providing authoritative guidance to organizations implementing electronic HIE. That guidance would help networks align with national standards and policies while responding to state, regional, and market conditions.

The report notes that the successful coordination of any privacy and security initiative would be affected by three factors: healthcare market geography, maturity of the state or local HIE initiative, and factors affecting cultural acceptance of a centralized governance model.

The report recommends that HHS work with state entities and interested national organizations to adopt, develop, and promulgate an HIE privacy governance infrastructure to consistently apply HIE privacy and security policies and business practices. It also recommends that HHS identify, analyze, and publicize the key HIE governance success factors.

## **Change a Patchwork to a Framework**

The report describes the existing federal and state laws and regulations that affect the privacy and security of electronic HIE as a “patchwork” of confusing, inconsistent, and inadequate laws and regulations. To lead the transition, the authors call for an organized state-led process to convert the patchwork into a consistent national framework.

The HISPC project found significant variation across all state teams in the interpretation and application of HIPAA rules and other federal laws and regulations relevant to HIE. State contractor stakeholder groups also raised the issue of the number of entities involved in HIE not covered under HIPAA and outside the reach of state-level regulation.

To resolve current confusion, misinterpretation, and misapplication of HIPAA and federal law the report calls for authoritative guidance that bears significant legal weight and extends adequate legal protections to covered entities.

In addition the report recommends that HHS assist states in establishing a privacy and security feedback mechanism that provides guidance to state entities facing questions regarding potentially ambiguous privacy and security situations under federal law. The proposed mechanism would be supported by the network of state organizations brought together by the HISPC research.

The report also recommends that the government:

- Produce and publicize collaborative state and federal guidance on report findings
- Create a single state organization to receive specific feedback and guidance from HHS agencies
- Produce and publicize use case scenarios for common problems

## **Develop Privacy Policy Guidance**

The report finds that the healthcare industry has failed to address privacy policy issues because of fear—fear of being out of compliance, fear of sanctions, fear of liability, fear of reputations lost. This failure results in overly conservative policies, complex solutions, and misinterpretation of laws, regulations, and policy.

One proposed solution is to convene a nationwide public-private effort to define a set of documents that serve as a baseline of common principle-based privacy and security policies, procedures, and standards to serve as a resource for all entities. The resource would be the result of a collaborative effort between federal and state governments. The creation of agreed-upon model policies, procedures, standards, and contracts would simplify and standardize implementation and resolve much of the variation that presently exists.

The state groups also identified a need for an Internet-based national privacy and security resource center that is easily accessible, efficiently searchable, and effectively used by industry.

## **Create Consumer Outreach, Engagement, and Education**

The project also found a need to reach out, engage, and educate stakeholders about electronic HIE and privacy and security issues. In order for HIE initiatives to succeed, they must engage and educate stakeholders about the significance of private and secure interoperable health information exchange.

Consumer engagement is necessary to build trust, which can be built upon formal outreach through community consultation. Effective community consultation processes must ensure that healthcare consumers be involved in the planning process at an early stage and remain engaged throughout HIE development.

Before a comprehensive education package is developed, it is critical to determine consumer understanding of current HIM practices and the privacy and security implications of moving to electronic health records and electronic health information exchange.

HIE initiatives must also make themselves known to consumer organizations. Engagement can be accelerated by reaching out to consumer groups. For these groups, health information exchange is generally perceived as a less pressing issue for which the payoff is comparatively remote. The healthcare industry must deliver a clear business case to consumer groups that electronic HIE will be a key driver for improving quality of care and reducing healthcare costs.

## HIM Professionals Contribute to HIE Success

As a direct result of these nationwide initiatives, action is being taken to facilitate communication and collaboration between the state and national privacy and security efforts. HIM professionals can contribute to the continued success of these collaborative initiatives by focusing their energies on increasing awareness, advocacy, and education.

**Harry B. Rhodes** ([harry.rhodes@ahima.org](mailto:harry.rhodes@ahima.org)) is director of practice leadership at AHIMA.

---

**Article citation:**

Rhodes, Harry B.. "Breaking Down Privacy and Security Barriers to HIE" *Journal of AHIMA* 78, no.10 (November 2007): 68-69.

---

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.