

# Modern Healthcare

THE ONLY HEALTHCARE BUSINESS NEWS WEEKLY

OCTOBER 6, 2009

## Guest Commentary: Start with common framework on IT security

**O**n Oct. 16, states will submit their health information exchange, or HIE, grant applications in order to receive their incentives under the American Recovery and Reinvestment Act of 2009.

The stimulus act essentially leaves each state to adopt its own information security and privacy framework for the protection of personal health information. Without a common language between states, healthcare organizations looking to connect across multiple HIEs will be subject to more regulations, ambiguity and audits that could lead to higher costs and complexities—effectively diminishing the aim of today's healthcare reform and resulting in no guarantee of greater trust in our healthcare system.

The first set of national standards for the protection of individually identifiable health information came to fruition with the enactment of the Health Insurance Portability and Accountability Act's privacy and security rules in 1996. But what was not broadly understood at the time of its enactment—and is still not understood by many today—is that the intent was to provide organizations flexibility in how they implement information privacy and security programs and was not intended to provide prescriptive guidelines for compliance.

Fast forward to 2009. Many organizations still misinterpret HIPAA for a variety of reasons, including ambiguity and lax enforcement. The healthcare IT portions of the stimulus act, originally found in a separate bill called the Health Information Technology for Economic and Clinical Health Act, or HITECH, does aim to address these issues with enhanced breach notification, clearer requirements in areas such as data encryption, extension of HIPAA to business associates and increased enforcement.

Compounding this issue is the fact that the stimulus act set aside \$23 billion for health IT with much of it earmarked for incentives to increase the adoption of electronic health records and connectivity through state HIEs.

Unfortunately, these exchanges present new issues and risks in the form of data protection and trust between organizations, consumers and government agencies. With the interconnectivity of the HIEs, the ability to trust the security mechanisms of an organization becomes even more vital. While there are national initiatives under way to ensure the interoperability of the exchanges, little has been accomplished nationally to ensure the HIEs and the organizations connecting to them are appropriately protecting sensitive health information.

The ambiguity of HIPAA has been a major driver in the increase in state regulations and requirements for healthcare organizations. For instance, Massachusetts already has defined an organization's responsibilities for protecting residents' personal health information, and California is moving to establish security requirements for any organization connecting to an HIE in the state. These are only two examples of what will soon be many as the State Health Information Exchange Cooperative Agreement Program, which establishes the guidelines for HIE incentives, requires the adoption of information security requirements by every state.

Our concern, supported by 45 states adopting their own breach notification requirements, is that healthcare organizations will be subject to myriad disparate, unclear data protection requirements and enforcement actions. While the complexity and inefficiencies are an issue, we understand the states' motivations and intentions for establishing these requirements.

As it stands, HHS' civil rights office has publicly stated its intention to



Daniel Nutkis

take a proactive approach on HIPAA privacy and security enforcement. It has also been communicated by the states that organizations should expect audits against state-specific information privacy and security requirements. State attorneys general have also been given the power to enact penalties in addition to those of the civil rights office.

Healthcare organizations are left without clear, consistent guidance with respect to information protection and a cost-effective approach to managing and reporting compliance. Managing the multitude of compliance requirements has always been a challenge, and the current path we are on will assuredly see an increase in time, money and manpower.

The good news is much of the industry understands its responsibility and has the desire to increase efficiency and keep health information private and secure. It is our strong belief the best method to secure health information is to give organizations the opportunity to proactively verify their compliance with federal and state privacy and security regulations.

Specifically, we believe organizations should have a vehicle through which to assess their level of information protection with a consistent approach to determine their compliance with various state and federal regulations. In turn, each organization can then report to a multitude of third parties, including the government, without the cost of multiple overlapping audits and reviews. Government agencies should identify an acceptable means to oversee and accept these certifications or attestations as sufficient evidence that an organization is in compliance.

As a first step, we recommend the industry adopt a common security framework, or frameworks, for compliance that encompasses the various federal and state regulations. This proactive approach will allow organizations to focus on the building blocks of security to achieve a state of compliance. One such option is the Health Information Trust Alliance's Common Security Framework, developed in collaboration with healthcare, business, technology and information security leaders and already widely adopted by healthcare organizations.

In addition, the framework, publicly available at no charge, has been selected or considered for adoption by a number of states to support their HIE information protection requirements. Regardless of which vehicle is adopted, much work is needed to ensure a consistent approach nationally.

It is also our belief that government agencies should take into consideration these proactive security efforts and focus their compliance actions—and attention—on organizations not demonstrating a commitment to improved security and privacy and those continuing to view information protection as a low priority.

As the broader healthcare reform debate looks at how to lower costs and create greater efficiencies, the industry needs to cooperate with the states to ensure information protection doesn't lead to unnecessary costs and increasing complexities. Moreover, as the public's trust in the protection of their health information decreases with the continued notification of security breaches, it is not evident that an increase in regulations and related audits equals greater information protection.

Daniel Nutkis, CEO  
Health Information Trust Alliance, Frisco, Texas

**HITRUST**  
Health Information Trust Alliance

www.HITRUSTalliance.net • info@HITRUSTalliance.net