Health insurerfocus

November 2011

A new data-sharing playground

The digitization of patient health information is inevitable, and so are the risks of compromising patient privacy.

From the Health Research Institute

Highlights

- Electronic health records, social media, secondary use of data, and mobile health are creating new opportunities for healthcare organizations, but headaches for privacy and security officers.
- On average, health insurers have experienced at least one privacy/security-related issue in the past two years, according to HRI research.
- More than 70% of healthcare executives surveyed said that recent breach enforcement actions have forced them to focus more on privacy and security.
- Old consent forms may not cover new data uses. Health insurers increasingly need to understand the permitted uses of data and the permissible channels of communication, and determine whether they have obtained appropriate consent.

As care and treatment become digitized and more easily shared, health insurers are facing these issues:

- **Access control of electronic health records (EHRs) and sharing of health information: "**Our policy restricts employees and physicians from accessing their own medical records, but there have been cases where curiosity gets the best of them," said one provider CEO. "Only *41% of health insurers reported including appropriate EHR use as a component of their employee privacy training.*
- **Risks with business associates**: "We have encountered vendors that have not worked with the healthcare industry before, so they have no idea about HIPAA (Health Insurance Portability and Accountability Act of 1996) requirements," said one health plan executive. "We have to help these prospective vendors become HIPAA compliant before we can work with them, and that becomes time intensive for us." *Healthcare organizations have only grazed the surface when it comes to ensuring their business associates can be trusted with protected health information (PHI). Only 45% of health insurers perform pre-contract assessments of their business associates and just 40% monitor post-contract compliance.*
- **Secondary data:** "Pharmaceutical companies are hopeful that the data available in EHRs will enable them to find more targeted candidates for clinical trials," said an attorney at a large pharmaceutical firm. "Our concern will be to protect privacy while expanding access to clinical trials." *Sixty-eight percent of health insurers said they are using or intend to use some form of secondary data, but only 57% have addressed or are in the process of addressing privacy and security.*
- **Virtual touchpoints**: "We need to meet the physician and patient needs and demands for mobile health and social media, but we are still focusing on how we manage the security implications," said the senior vice president of IT services at a large health system. *Nearly half (55%) of healthcare organizations have not addressed the privacy and security of mobile devices, according to the PwC survey. Less than 50% of organizations surveyed have included the approved uses of social media and mobile devices in company privacy training.*

pwc

Data use (privacy) and data protection (security)
Safeguards are not keeping pace with an explosion of communication channels and data uses

The digitization of patient health information is inevitable, and so are the risks of compromising patient privacy. As medicine becomes increasingly personalized through greater access to information mined from new data assets, business opportunities are starting to entice health insurers to engage with other health sectors on a new data-sharing playground.

But, there are barriers to gaining admission. Among them is the reality that privacy and security safeguards are not keeping pace with the need to increasingly protect personal information from the bullies. For example, old forms of consent may not cover new data uses.

To understand how healthcare organizations are coping with security and privacy challenges, PwC's Health Research Institute surveyed more than 600 provider, health insurer, and pharmaceutical/life sciences professionals on the privacy and security implications of the explosion of new data sources and uses in the health industry. HRI also interviewed 25 chief privacy officers (CPOs), chief information security officers (CISOs), chief information officers (CIOs), and other executives of healthcare organizations.

According to the HRI survey, 54% of healthcare organizations surveyed by PwC said they had experienced some type of privacy and security-related issue over the last two years. Hospitals were more likely to report a privacy/security-related issue than health insurers or pharmaceutical/life science companies (1.5 issues in the last two years compared to 1.1 and 0.7, respectively).

PwC's research found that there is considerable concern for the "knowledgeable insider." Improper use of protected health information (PHI) by an internal party was the leading privacy/security issue experienced by healthcare organizations over the last two years, according to the HRI survey. Improper file transfer containing PHI and transfer of PHI to an unauthorized party were top issues reported by health insurers.

HRI asked health insurers the following question: **Within the last two years, which of the following have you experienced?**

- Improper use of PHI by an internal party: 17%
- Patients seeking services under others' names: 16%
- Improper file transfer containing PHI: 25%
- Transfer of PHI to an unauthorized party: 21%
- Security breach of PHI: 9%
- Improper use of PHI by an external party: 16%
- Financial ID theft: 5%

Source: PwC survey

Employers and consumers are looking for more value from the health system. As a result, provider, payer, and pharmaceutical/life sciences sectors are starting to converge and work together in new data sharing arrangements and care delivery models that make them accountable to the patient.

However, PwC's survey showed that most healthcare organizations are not yet participating in external data exchange. Pharmaceutical and life sciences companies are most likely to participate (61%) and health insurers and providers are far less likely to participate (40% and 38%, respectively).

Still, the future points to more sharing. EHRs are becoming increasingly interoperable and more hospitals and health insurers are joining health information exchanges (HIEs). They also are creating larger consolidated databases of health data to participate in accountable care organizations (ACOs), initiatives, or collaborations, and to create business opportunities.

But, one of the most vexing issues for health insurers is ensuring their business associates can be trusted with personal information. Of the 11 million people affected by reportable data breaches between September 2009 and June 2011, 6 million, or 55%, were affected by data breaches involving business associates, according to the federal government. Less than half of health insurers are taking steps beyond the business associate agreement to protect sensitive data.

HRI asked health insurers the following question: **In which ways do you ensure that a business associate can be trusted with PHI?**

Business associate agreement	74%
Pre-contract assessment	45%
Post-contract compliance assessment	40%
Require business associates to become HITRUST certified	11%

Source: PwC survey

Unfortunately, there is no single, commonly used framework for assessing business associates. Recently, the Health Information Trust Alliance (HITRUST) established the Common Security Framework, a certifiable framework for organizations that create, access, store, or exchange personal health and financial information.

Questions and answers

Q: How can my organization develop the right strategy to address both privacy and security?

A: By adhering to the following four guidelines, health insurers can address these issues strategically:

- **Integrate privacy, security, and compliance approaches and frameworks**
- **Make minimum controls and standards a prerequisite to play**
- **Deputize all workers as privacy champions**
- **Make privacy part of the consumer experience and brand**

Q: How common is it for health insurers to have an integrated approach?

A. Among health insurers, 82% said they have integrated, at least to some extent, their approaches to compliance, privacy, security, and identity theft. Only 46% said they have done so to a great extent. The HRI survey found that organizations that have integrated approaches to a great extent have seen distinct benefits. They are:

- More likely to believe the security of their data has increased over the past year.
- More likely to have increased staffing in the privacy and security areas.
- Less likely to have experienced privacy/security-related issues in the last two years.

Health insurers saw the largest difference in the number of privacy and security issues reported in the last two years among those that had highly integrated approaches and those that did not (0.8 issues, compared to 1.3).

Q: How do I know if my organization is complying with the new regulations?

Current privacy and security regulations do not specify how an organization can achieve compliance. For example, HIPAA regulations require that organizations secure information shared via portable mobile devices, but do not explain how this should be done. As a result, organizations should consider breaking down compliance to the least common denominator. Some organizations are developing minimum guidelines for data protection that are agnostic to the privacy regulations, because there is a great deal of personal data that falls outside of HIPAA but still requires protection and because required levels of protection vary among regulatory bodies. For example, state laws do not define encryption, but the HITECH regulations do, based on the National Institute of Standards and Technology (NIST), government standards, and other standards that healthcare may not have looked to prior to HITECH.

Leveraging standards will help to eliminate the gaps in regulations. Also, it's not just about compliance; it's about managing risk and improving overall operational performance.

Q: How can we create a culture of confidentiality among our employees?

A: Privacy and security initiatives should be incorporated into each business unit, with centralized oversight. Good training can enable employees and physicians to make decisions regarding the protection of patient data without making them afraid to do their jobs.

Contact information

For a deeper discussion, please contact

Peter Harries
Principal
PwC
(213) 356-6760
peter.harries@us.PwC.com

Jim Koenig
Director
PwC
(267) 330-1537
james.h.koenig@us.PwC.com

Nalneesh Gaur
Director
(214) 754-5232
nalneesh.gaur@us.PwC.com

To read more, download the HRI report, *Old data learns new trick: Managing patient privacy and security on a new data-sharing playground*

pwc.com/hri

pwc.com/us/healthindustries

twitter.com/PwCHealth