

Old data learns new tricks

Managing patient privacy and security on a new data-sharing playground

Health Research Institute

September 2011

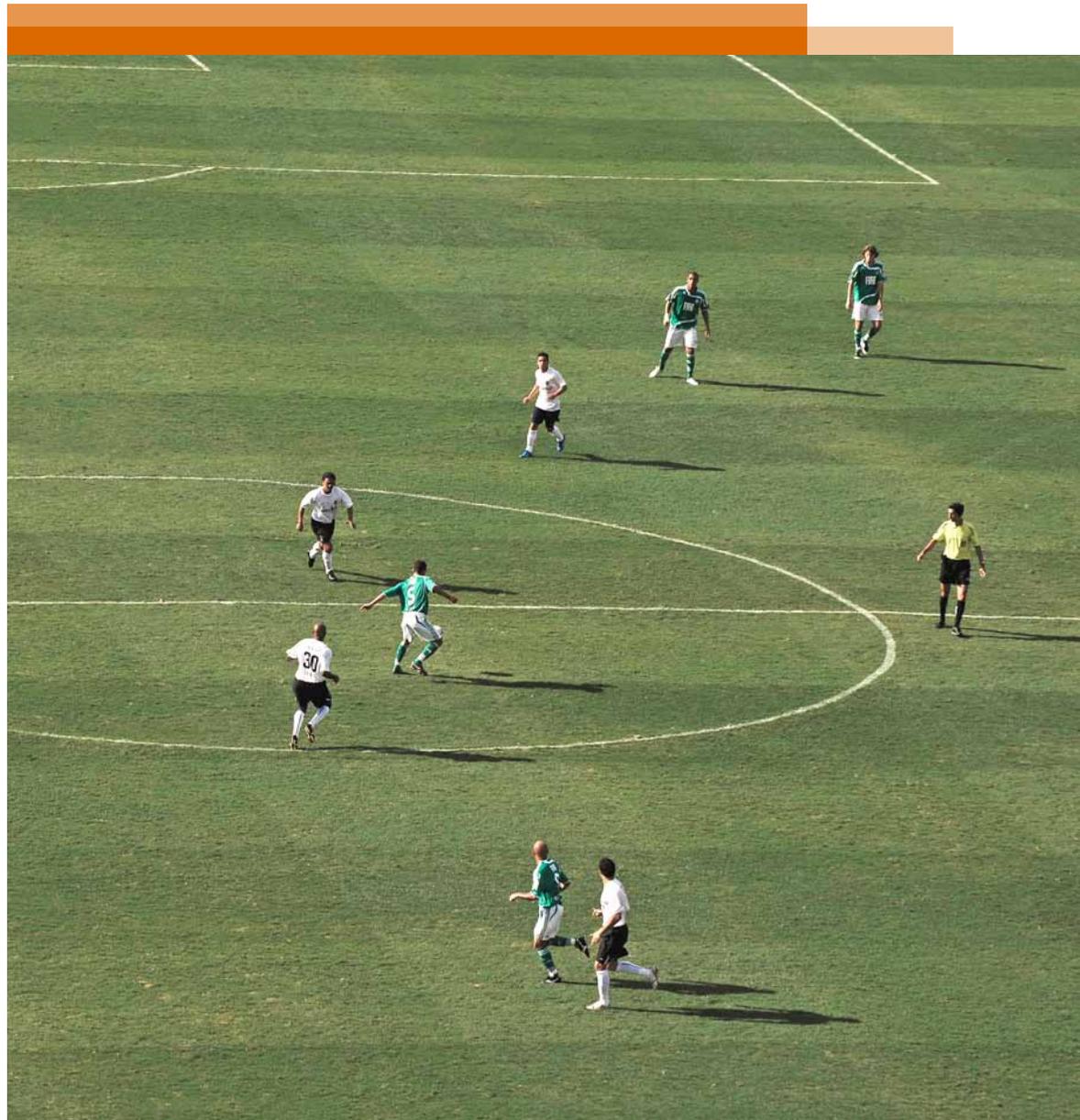


Table of contents

The heart of the matter **2**

Securing data and protecting privacy are critical as the health industry converges in a new data-sharing playground

An in-depth discussion **4**

Digital health is becoming both a data-sharing playground and a minefield of concerns

Executive summary	5
The data-sharing playground	7
New privacy and security challenges	9
1. Data use	9
2. Data protection	11
Four factors driving health sectors to revisit their privacy and security practices	14
1. Access in EHRs and sharing of health information	14
2. Business associates	16
3. Secondary data use	20
4. Virtual touchpoints	23

What this means for your business **27**

Common strategies for healthcare organizations to move forward

Integrate privacy and security approaches	28
Make minimum controls and standards a prerequisite to play	30
Deputize all workers as privacy champions	32
Make privacy part of the consumer experience and brand	33

The heart of the matter

Securing data and protecting privacy are critical as the health industry converges in a new data-sharing playground

Data is quickly becoming one of the health industry's most treasured commodities. The United States is embarking on the largest investment in health information technology (IT) ever with high hopes of improving patient outcomes, quality, and costs. New data assets, care approaches, and payment models are on the horizon, generating an explosion of information collection, exchange, and use in the industry. Yet, health organizations are acutely aware that sensitive data can be easily compromised. In just the last year and a half, a breach of personal health information occurred, on average, every other day.¹ Breaches erode productivity and patient trust. They're costly, unpredictable, and unfortunately quite common. More than half of healthcare organizations surveyed by PwC have had at least one privacy/security-related issue in the last two years.

On one hand, the government is encouraging organizations to share data more broadly to improve outcomes, but at the same time imposing larger penalties for improper disclosures. As a converging industry moves quickly to tap the torrents of new electronic data available, PwC's Health Research Institute (HRI) found that the challenges are complex, but manageable.

For this research, HRI 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 healthcare industry. HRI also interviewed 25 chief privacy officers (CPOs), chief information security officers (CISOs), chief information officers (CIOs), and other executives of healthcare organizations.

¹ US Department of Health and Human Services Office for Civil Rights, accessed June 27, 2011, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>.

An in-depth discussion

Digital health is becoming both a data-sharing playground and a minefield of concerns

Executive summary

As every aspect of care and treatment becomes digitized and more easily shared, health organizations are facing an array of privacy and security challenges. The most frequently reported issue among providers was the improper use of protected health information (PHI) by an internal party, and improper file transfer containing PHI among health insurers and pharmaceutical and life sciences companies. Pharmaceutical and life sciences respondents appeared least aware about these issues—64% saying they did not know if their organization had experienced a privacy/security-related issue in the last two years.

Following are concerns voiced by healthcare executives and what our PwC survey research told us about these concerns:

- **Access in 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 Thomas J. Lewis, president and chief executive officer at Thomas Jefferson University Hospitals, Philadelphia. “Our current stance is that our employees and physicians should not have any special access to their records that the average patient does not have.”
 - Only 58% of providers and 41% of health insurers reported including appropriate EHR use as a component of their employee privacy training.
 - Of the healthcare organizations that are sharing data externally (45%), only one-quarter have executed data sharing agreements with all participants.
- **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 Hope Scott, senior privacy counsel at CIGNA. “We have to help these prospective vendors become HIPAA compliant before we can work with them, and that becomes time intensive for us.”
 - Of the 11 million people affected by data breaches since September 2009, 55% were affected by data breaches involving business associates.
 - Healthcare organizations have only grazed the surface when it comes to ensuring their business associates can be trusted with PHI. Only 38% perform pre-contract assessments of their business associates and just 26% conduct post-contract compliance assessments.
- **Secondary data:** Organizations are now using their health data for secondary uses, such as clinical studies outcome-based research, and post-market surveillance of drugs.
 - Nearly three-quarters of healthcare organizations PwC surveyed said they are using or intend to use some form of secondary data, but less than half have addressed

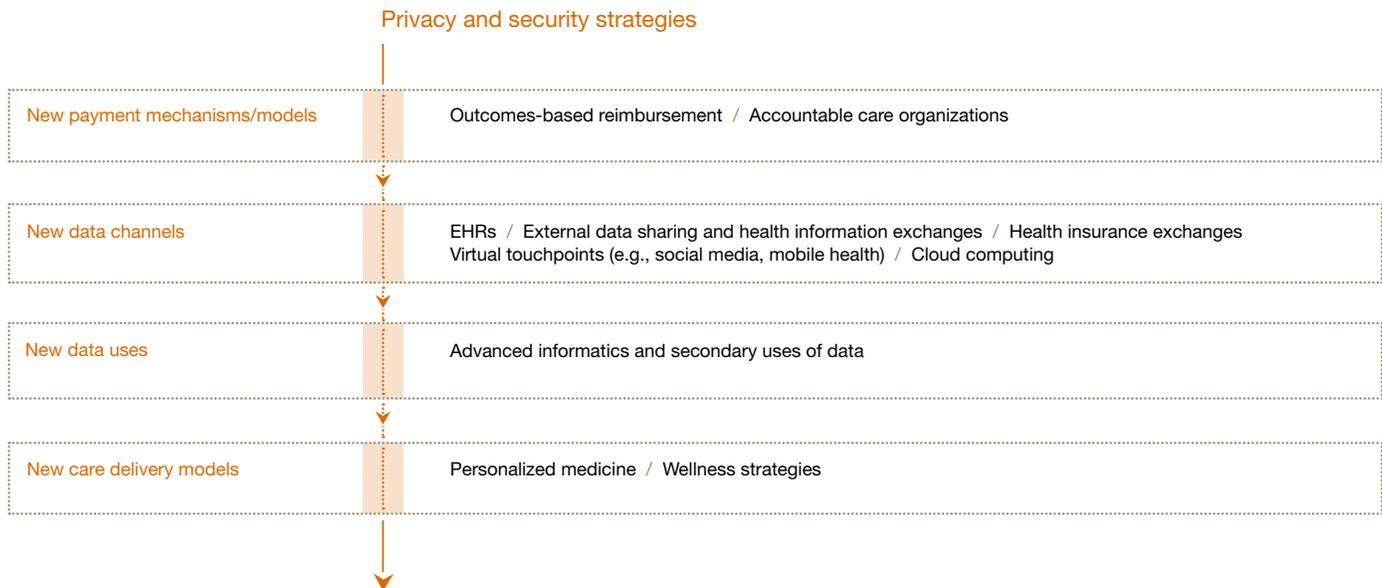
The digitization of patient health information is inevitable, and so are the risks of compromising patient privacy.

- or are in the process of addressing privacy and security. Providers are most likely to participate.
- Top challenges mentioned were establishing information security functions, appropriately encrypting data, and creating multiple levels of separation between the data and the end consumer.
- **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. There is a direct correlation between the level of mobility and our ability to protect that data,” said Luis Taveras, senior vice president of information technology services at Hartford HealthCare Corp., an 867-bed major teaching facility in Connecticut.
 - Privacy and security concerns regarding the proliferation of mobile devices may slow progress towards work efficiency and flexibility. 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 noted that they have included the approved uses of social media and mobile devices in company privacy training, according to the PwC survey.
- Pharmaceutical/life science companies were more likely than providers and health insurers to report social media as a top privacy/security concern (35% compared to 27% and 21%, respectively).
- Privacy concerns may be holding back many healthcare organizations from using social media to connect with patients and consumers. Less than one-fourth of survey respondents said they have already addressed the privacy and security implications of social media.

While each industry sector has specific privacy and security issues—four guidelines provide a common strategy for providers, health insurers, and pharmaceutical/life sciences firms to move forward in this environment:

- 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

Figure 1: Regulatory and market pressures drive an expansion of data channels and create new data uses to enable emerging care models.



The data-sharing playground

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 all health sectors to engage 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.

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 care delivery models that make them accountable to the patient.

Historically, healthcare has been programmed to deliver symptom-based rather than preventive care. New technologies are now enabling a gear shift to personalized medicine—treatment focused on the individual—to facilitate a movement from the treatment of disease toward wellness and prevention.

Advances in genetic research have made personalized diagnostics and treatments possible, for example, through pharmacogenetics that examine the relation of genetic factors to variations in responses to drugs. New technologies, payment mechanisms, and regulatory pressures have planted the seed for new care delivery models that focus on improving quality and outcomes while reducing cost. Also, consumers are looking for more convenience in the health system and to become more engaged in monitoring their own health, so many components of healthcare are moving outside of traditional settings with

increased use of wireless and broadband technologies that empower them through use of mobile devices, remote monitoring, and mobile applications on smartphones.

In 2010, providers alone spent more than \$88.6 billion on health IT initiatives in response to the US government’s “meaningful use” incentive program to drive widespread adoption of electronic health records (EHRs).²

As EHRs become interoperable and health information exchanges (HIEs) form, organizations are submitting more and more data, creating larger consolidated databases of health data to participate in accountable care organizations (ACOs), initiatives, or collaborations, and to create business opportunities. (See Figure 1).

² Kenneth Brant, *Forecast: Enterprise IT Spending by Vertical Industry Market, Worldwide, 2008-2014, 1Q10 Update*, Gartner, April 30, 2010.

Nearly three-quarters of healthcare organizations PwC surveyed said they are using or intend to use some form of secondary data.

These new data assets and channels and others—like social media—are generating the need for advanced informatics to better understand the effectiveness and uses of drugs, tests, and courses of treatment. “Pharmaceutical companies are hopeful that the data available in EHRs will enable them to find more targeted candidates for clinical trials,” said Debra Bromson, senior counsel, commercial and privacy, at AstraZeneca Pharmaceuticals. “Our concern will be to protect privacy while expanding access to clinical trials.”

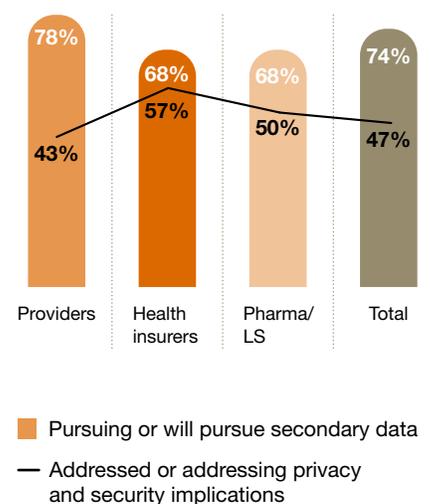
Each health sector has a vested, albeit slightly different, interest. For example, pharmaceutical companies want richer outcomes-based research to prove that *their* drugs are the most effective on the market, while health insurers are interested in accessing a broader spectrum of patients to identify *which* drug is the most effective. Some pharmaceutical companies have also found new value in using claims data to identify geographic hotspots that might be at risk for increased off-label marketing of drugs.

One emerging trend in this environment is the use of secondary health data—data that is used for a purpose other than to treat a patient. Nearly three-quarters of healthcare organizations PwC surveyed said they are using or intend to use some form of secondary data—up from 65% two years ago³, as they start to turn data into actionable information that can guide the development of new products, mitigate risk,

change the behavior of patients and clinicians, and determine the effectiveness of care and treatments. But demand for secondary data uses among the health sectors has outpaced the implementation of necessary privacy and security safeguards—only 47% of survey respondents said they have addressed or are addressing the privacy and security implications of secondary data use. (See Figure 2).

Monetization of data will drive new business models (See Figure 3) and create revenue sources that will result in measurable advances in quality of care for patients and their families, and improve the health status of societies—but only if data ownership, dissemination, and patient privacy and security issues are addressed first.

Figure 2: Secondary data use across the healthcare sectors.



Source: PwC Health Research Institute Privacy and Security Survey, 2011

³ Transforming healthcare through secondary use of health data, PricewaterhouseCoopers 2009.

New privacy and security challenges

As the health industry converges in a new data-sharing playground healthcare organizations will need to assess the trade-offs between protecting privacy and the quality of information leveraged from individually identifiable health data. This requires close collaboration and sharing of accountability between privacy and security functions, as the boundaries between privacy and security start to blur in response to the privacy laws and regulations themselves blurring. Healthcare organizations need an understanding of the two driving facets of privacy and security today:

- 1. Data use (privacy):** For years, laws have restricted how healthcare organizations can interact with

consumers, trial subjects, healthcare professionals, and business-to-business partners, and have limited the uses of health and other personal data in various channels of communication (e.g., email, Internet, social media, mail). There are now more than 200 laws in more than 150 countries addressing data privacy. And, in the United States, many states have their own rules governing the types of consent needed for the use of individual health data for marketing, research, and other purposes.

The challenge for healthcare organizations in this new health information economy is that old forms of consent may not cover the new data uses or new channels of

communication. Either new consent has to be obtained or the information cannot be used for the intended purpose or in the new channels. (See sidebar: *Consumers want to know: Who knows what about me?*) As a result, healthcare organizations increasingly need to understand the permitted uses of data and the permissible channels of communication, and determine whether they have obtained the appropriate consent to cover new and secondary uses, new interactions, and direct communication channels.

Figure 3: Potential partnerships and uses for secondary data.



Source: Emerging Economy of Data breakout session, PwC 180° Health Forum, 2010.

Consumers want to know: Who knows what about me?

Patient privacy notices are evolving as organizations increase secondary data use and business associate relationships. Consumers need to be made aware of how their data is being disseminated.

Consider the following example:

Stage 1: Health plan sponsors a wellness fair. The health insurer is required to communicate to workers that their employer will be notified of their participation.

Stage 2: An outside vendor is hired by a health plan to manage the health fair. The plan must inform the worker that the vendor also has the participation information.

Stage 3: The vendor may receive a worker's biometric results for use in outcomes research.

This type of sharing can raise alarms for consumers. "We need to start talking to our customers holistically about the benefits of sharing their health information," said CIGNA's Scott. CIGNA's Customer Experience Department has implemented a campaign called "The Words We Use," which eliminates the jargon and requires CIGNA to communicate with consumers in a more direct and transparent way.

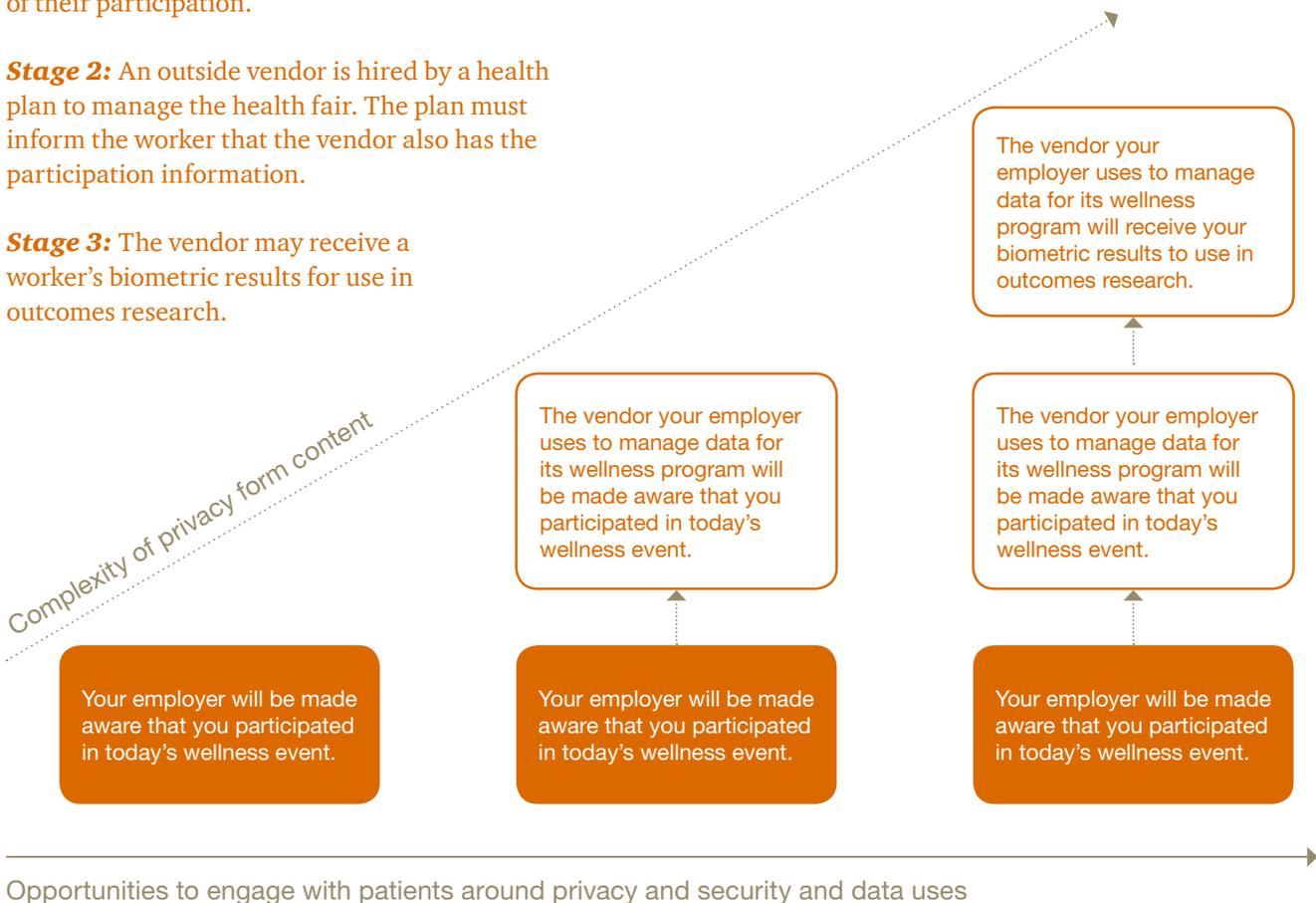
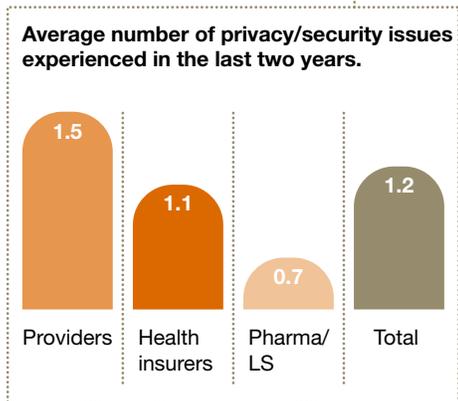
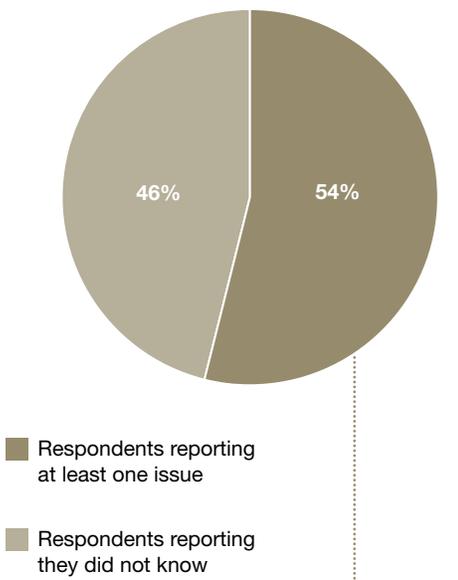


Figure 4: Healthcare organizations that have experienced a privacy/security breach in the last two years.

In the last two years, has your organization experienced a privacy/security-related issue?



Source: PwC Health Research Institute Privacy and Security Survey, 2011

2. Data protection (security): There has been an increase of regulator focus on data protection controls and there are new notification requirements for breaches that place them in the public eye. United States federal and state regulators are aggressively inspecting and pursuing privacy breaches and the absence or failure of data safeguards. In the US, the criminal and civil penalties imposed on organizations that have experienced a breach are a revenue source to fund the government’s stimulus incentive program to drive widespread EHR adoption. The US Department of Health and Human Services Office for Civil Rights (OCR) has also ramped up desk audits and remediation demands, making case examples of organizations that have never even had a breach. Audit and enforcement activity is sure to continue. More than 70% of healthcare executives surveyed said that recent breach enforcement actions have forced them to focus more on privacy and security.

According to a survey PwC conducted in spring 2011, 54% of respondents said they were aware that their organization had experienced some type of privacy and security-related issue over the last two years. (See Figure 4). 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).

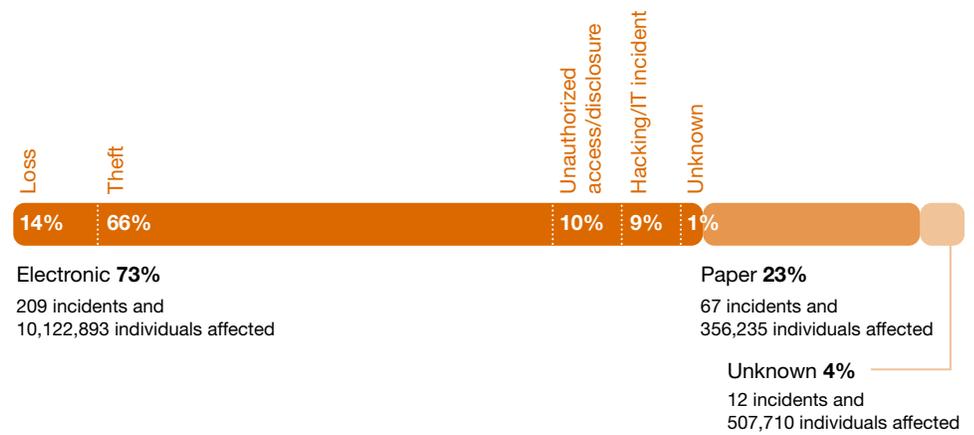
Almost half of executives surveyed said they were not aware—or possibly not willing to report—that a privacy/security issue had occurred at their organization in the last two years. Pharmaceutical and life sciences respondents appeared least aware about these issues—64% said they did not know if their organization had experienced a privacy/security-related issue in the last two years. Since September 2009, 288 breaches have been reported to OCR.⁴ That’s more than one reported breach every other day; 11 million individuals have been affected to varying levels.⁵ The Ponemon Institute, a company that conducts independent research on privacy, data protection and information security, estimated the average economic impact of a data breach over a two-year period to healthcare organizations at \$2 million.⁶ Certainly, the impact to brand and reputation can be farther-reaching.

4, US Department of Health and Human Services Office for Civil Rights, accessed June 27, 2011, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>.

6 Ponemon Institute LLC, Benchmark Study on Patient Privacy and Data Security, November 9, 2010, <http://www2.idexperts.com/resources/healthcare/healthcare-articles-whitepapers/ponemon-benchmark-study-on-patient-privacy-and-data-security/>.

Keeping track of “who has access to what” in a constantly changing and expanding enterprise is an extremely difficult and risky mission.

Figure 5: Electronic versus paper breaches impacting over 500 individuals (since September 2009).



Source: US Department of Health and Human Services Office for Civil Rights, accessed June 27, 2011, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>.

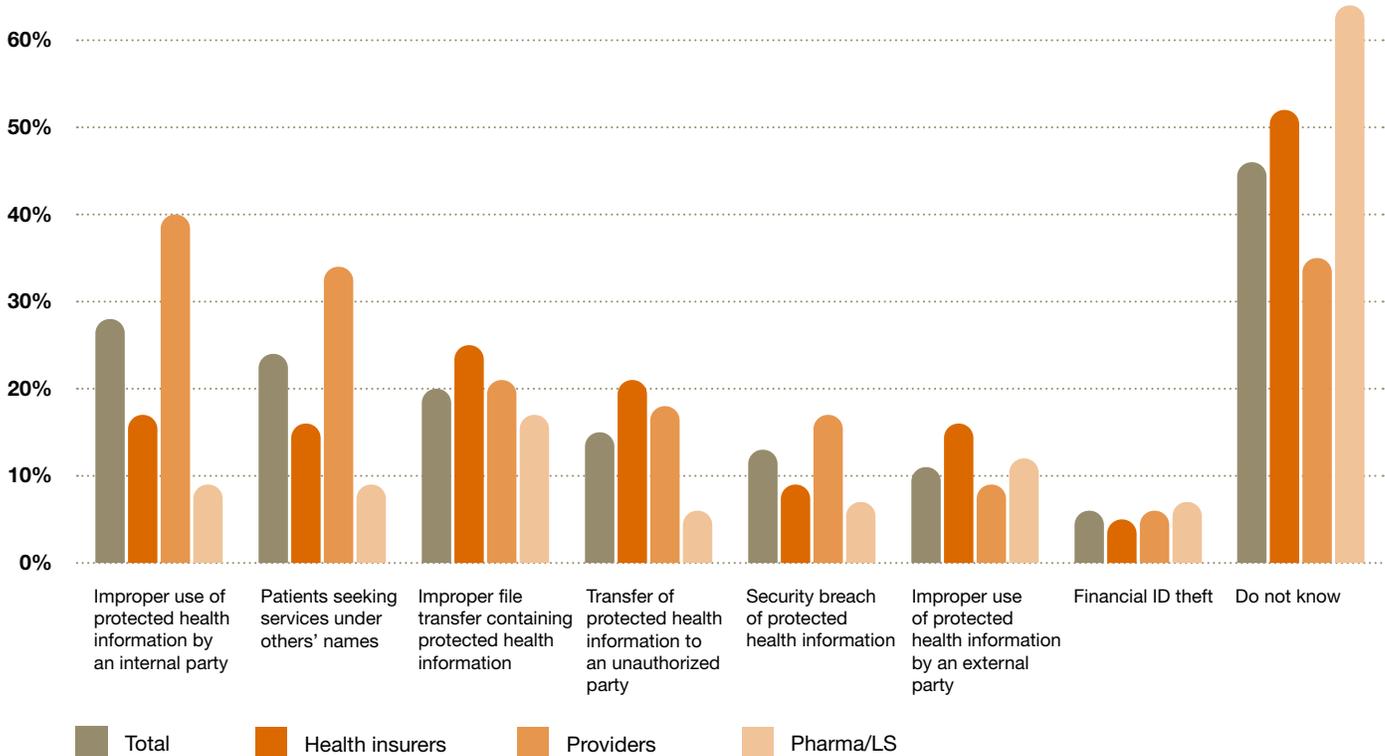
While electronic data breaches occurred three times more frequently, paper-based breaches are still on the radar and, according to interviews, a large concern for healthcare organizations. Electronic mode of data transmission and storage allows organizations to more easily manage data security, but electronic data breaches have a further-reaching impact—on average, approximately 48,000 individuals were affected per electronic data breach, compared to just over 5,000 per paper-based breach.⁷ (See Figure 5). Most electronic data breaches, though, do not result from hacking or an IT-related incident. In fact, the largest data leak in the United States had nothing to do with technology. Of the electronic data breaches reported to OCR, 90% were a result of a lost computer or device, theft, or unauthorized access/disclosure. “Many compliance officers are most

concerned about IT breakdowns and hackers,” said Roy Snell, chief executive officer and co-founder of the Society of Corporate Compliance and Ethics and Health Care Compliance Association. But, breaches can result easily from—and with greater probability—mishandling of paper documents, people talking in the elevator, or comments made via social media channels. “The IT department should be heavily involved from a software standpoint, but organizations need to understand that the real problem may be the person standing right next to them,” he said.

⁷ US Department of Health and Human Services Office for Civil Rights, accessed June 27, 2011, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>.

Figure 6: Privacy/security issues experienced by healthcare organizations over the last two years.

Within the last two years, have you experienced any of the following? Please select all that apply. (all respondents)



Source: PwC Health Research Institute Privacy and Security Survey, 2011

PwC’s research found that there is considerable concern for the “knowledgeable insider.” Improper use of 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. (See Figure 6).

Theft accounted for 66% of total reported data breaches since 2009. Medical identity theft is the fastest growing form of identity theft. Over one-third of providers PwC surveyed said that they have experienced patients seeking services under another person’s name. The Ponemon Institute estimated that 1.42 million Americans were affected by medical

identity theft in 2010, with a total economic impact \$28.6 billion.⁸ Victims of medical identity theft are left with large, unpaid medical bills, damage to their credit, and potentially worse—like medical treatment recommendations based on someone else’s health information.

Following, we highlight four privacy and security challenges health sectors face in the new health information economy.

⁸ Ponemon Institute LLC, Second Annual Survey on medical identity theft, March 2011, accessed July 21, 2011.

Four factors driving health sectors to revisit their privacy and security practices

1. Access in EHRs and sharing of health information

Across the board, healthcare organizations agree on two of their top three security challenges: (1) end-user access controls and identity management and (2) encryption of data in storage and in transit. (See Figure 7).

Access controls

In a paper world, patients' medical records needed to be physically stored and locked and medical records could be accessed by only one person at a time. Now, as more stakeholders enter onto the playground through digitized records and health databases, organizations need to build more granular access control models to prevent overexposure of information. Historically, however, this has been an area of underinvestment in healthcare since HIPAA's minimum-necessary rule required covered entities to implement only broad access procedures. The rule called for granting role-based access to classes of persons that needed access to the information to carry out their job duties, identifying categories or types of PHI needed, and including conditions appropriate to such access. Case-by-case review of each was not required.

The traditional model of defining roles and responsibilities, managing user access, and granting authorization is not working. User identities and privileges stored in multiple applications and repositories across the enterprise have resulted in control deficiencies. And as databases continue to expand as data from EHRs is shared in HIEs and ACOs and with business associates, it becomes increasingly difficult to keep track of who has or should have access to what. Organizations need a centralized and comprehensive view of people, roles, and privileges for more accurate and efficient auditing and reporting, and for continuous improvement of policies and controls. In a recent PwC survey of health systems, half of respondents said that they would apply for the government's "meaningful use" incentives in 2011,⁹

but only 19% said they have completed the prerequisite security assessment that includes criteria for access control, identity management, and encryption.

External data sharing

PwC's survey showed that most health-care organizations are not participating in external data exchange now. Pharmaceutical and life sciences companies are most likely to participate (61%) and health insurers and providers are nearly equally as likely to participate (40% and 38%, respectively). (For more information on health information exchanges and ACOs, see *Designing the health IT backbone for ACOs*.)

⁹ Putting patients into "meaningful use", PricewaterhouseCoopers Health Research Institute, 2011.

Figure 7: Top three security challenges by health sector.

Providers	Health insurers	Pharmaceutical/life sciences
<i>EHR/PHR access controls and identity management (81%)</i>	<i>EHR/PHR access controls and identity management (58%)</i>	Document retention compliance (56%)
<i>Encryption in storage and in transit (57%)</i>	<i>Encryption in storage and in transit (52%)</i>	<i>Encryption in storage and in transit (42%)</i>
Required software upgrades (28%)	Alternative identifiers and information masking (34%)	<i>End-user access controls and identity management (41%)</i>

Italic: Denotes challenges in common.

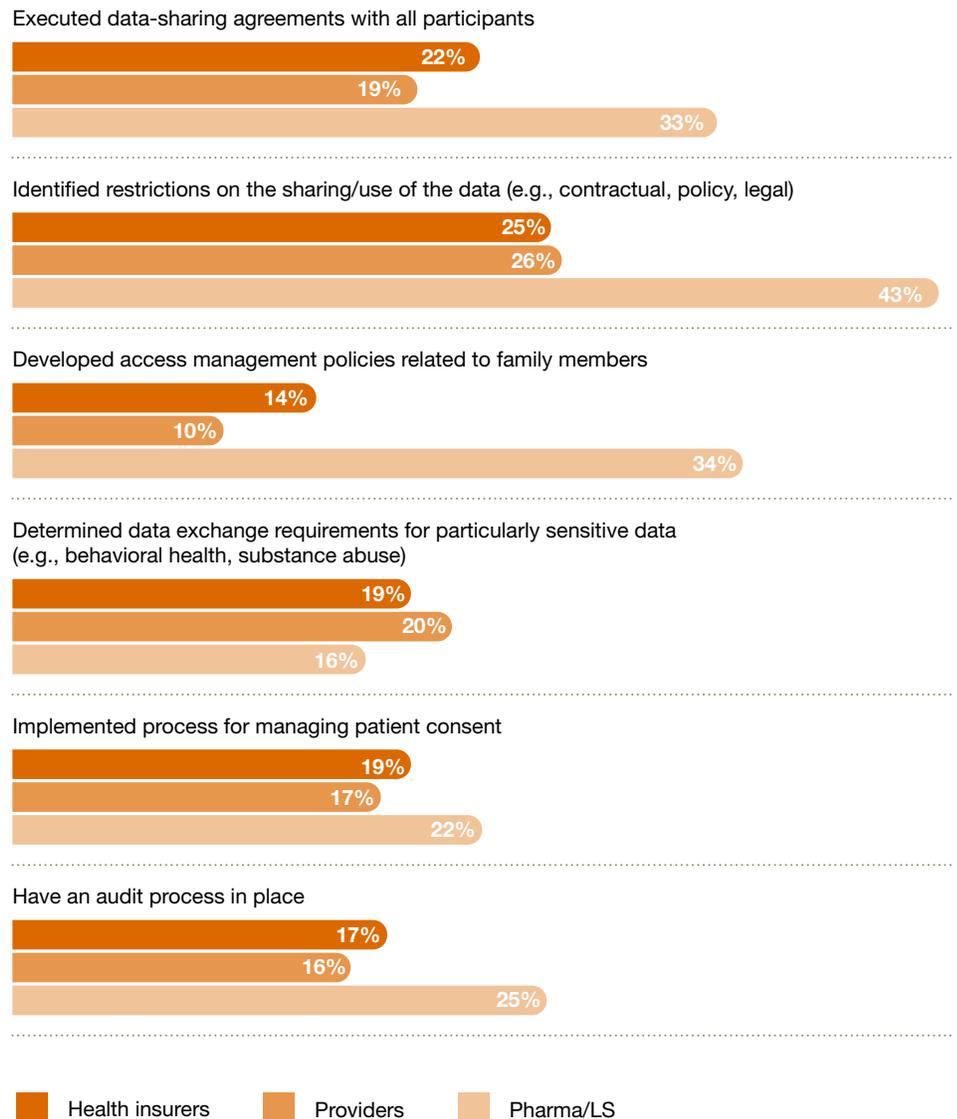
Source: PwC Health Research Institute Privacy and Security Survey, 2011

But on average less than one-third of the organizations that are sharing externally said they have identified restrictions on data-sharing and use or executed data-sharing agreements with all participants. Fewer have figured out how they will manage patient consent and access control for patients' family members or designees (except pharmaceutical/life science companies), or how they will audit data sharing. (See Figure 8).

Cross-border data transfers are also becoming a challenge. Unlike business-conduct laws that are required to conduct business in another state or country, privacy laws are consumer protection laws, so the protection travels with the patient. For example, if a patient from Massachusetts receives treatment in a healthcare facility in Utah, the facility must comply with Massachusetts privacy laws. Providers need to rethink how they comply with privacy laws and not limit their focus to HIPAA requirements. International data transfers are a particular concern for global health insurers and pharmaceutical and life sciences companies conducting clinical trials internationally, because there is virtually no consistency of data protection agreements, many times not even within the same company. Some countries have restrictions on data transfer to countries that have lesser protections by law.

Figure 8: Activities healthcare organizations have completed for external data sharing.

If you are currently sharing data externally, which of the following activities has your organization completed? Please select all that apply.



Source: PwC Health Research Institute Privacy and Security Survey, 2011

“There is a general lack of education about the requirements of business associates. Few organizations are able to truly monitor or assess the business associates’ privacy and security practices.”

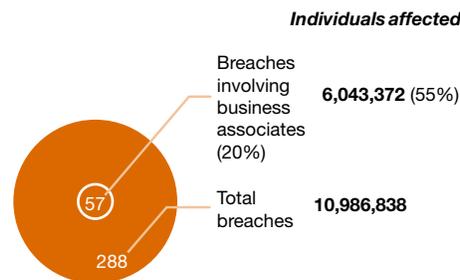
– Kimberly Gray, IMS Health

2. Business associates

Of the 11 million people affected by data breaches since September 2009, 6 million, or 55%, were affected by data breaches involving business associates (partners/vendors).¹⁰ (See Figure 9).

Under the HITECH Act, business associates with whom healthcare organizations share PHI must now comply with the HIPAA Privacy and Security Rules and are subject to the same enforcement measures as covered entities. (See sidebar: *Privacy rules stemming from HIPAA and ARRA/HITECH regulations*).

Figure 9: Breaches involving business associates.



Source: US Department of Health and Human Services Office for Civil Rights, accessed June 27, 2011, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>

For healthcare organizations that entrust material amounts of highly sensitive PHI to external parties, an emerging industry trend, especially among health insurers, is to assess the privacy and security practices of their business associates primarily through interviews and/or questionnaires. In fact, in Massachusetts companies are required to assess the privacy and security capabilities and regulatory compliance of vendors that have been entrusted with personal information, as defined by state law.¹¹

But, healthcare organizations appear to have only grazed the surface when it comes to understanding the privacy and security practices of their business associates. According to the survey, most organizations require only a business associate agreement, while only 38% perform pre-contract assessments of their business associates. Commonly,

¹⁰ US Department of Health and Human Services Office for Civil Rights, accessed June 27, 2011, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>.

¹¹ MA CMR 201 § 17.03(2)(f)(2) provides that among other requirements that companies must take “reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information [in paper or electronic form] consistent with [MA CMR 201 § 17.00 et. al] and any applicable federal regulations,” including HIPAA/HITECH. It should also be noted that MA CMR 201 § 17.00 et. al applies to companies and other persons “who own or license personal information about a resident of the Commonwealth of Massachusetts,” not just companies that have operations in Massachusetts.

Privacy rules stemming from HIPAA and ARRA/HITECH regulations

To embed privacy throughout an organization, it's important to understand the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the American Recovery and Reinvestment Act of 2009, which included the Health Information Technology for Economic and Clinical Health (HITECH) Act. HIPAA was enacted to establish consistent industry standards to ensure the privacy and security of personal health information and personal medical records. The HITECH Act was established to promote the digitization of data and transmission of information across the healthcare industry and expand HIPAA by imposing new privacy and security requirements.

HIPAA Privacy Rule

- Covers unauthorized disclosure of any personal health information
 - Requires consent/authorization for access sharing or uses of personal health information
 - Requires delivering notices and honoring choice (opt-out)
 - Requires "business associates" to enter agreements and account for disclosures
-

HIPAA Security Rule

- Covers protection of electronic personal health information only (not paper records)
 - Provides regulated controls: 42 required and addressable items like policies and access controls (e.g., complex passwords, authentication, user provisioning and ID management), monitoring, physical security, secure networks, encryption in storage and transit)"
-

HITECH Act

- Requires breach notifications to be sent to individuals, the Department of Health and Human Services, and media to disclose unauthorized access and breaches of "unsecure" personal health information
- Requires business associates to fully comply with HIPAA Privacy & Security Rules
- Imposes criminal penalties for companies and individuals (including employees) and requires civil penalties for violations
- Increases electronic health records privacy and security requirements beyond HIPAA for personal health information stored in, or created by electronic health records

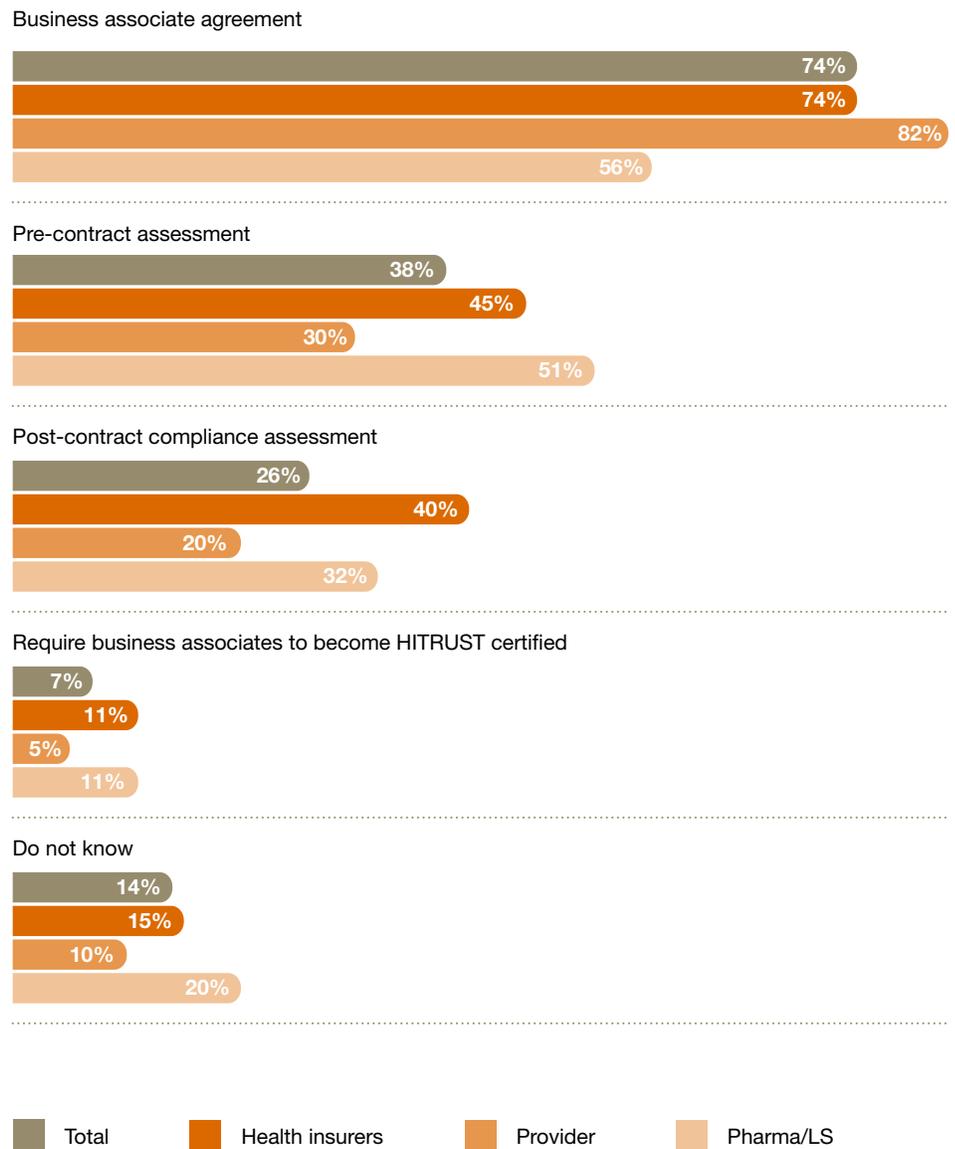
these assessments include questionnaires and interviews regarding a minimum set of standards organizations require of their business associates (as outlined later in this report), rather than testing of IT systems. Just 26% said they assess compliance with contract terms related to privacy and security (e.g., requesting confirmation that the vendor has destroyed PHI following expiration of the contract). (See Figure 10). Providers appear less likely than health insurers and pharmaceutical and life sciences companies to do either.

Interviews PwC conducted supported the survey findings. “Business associates are the most misunderstood area for the healthcare industry,” said Kimberly Gray, global chief privacy officer at IMS Health, the leading provider of information services for the healthcare industry. Gray, who previously performed in a similar role at a large regional health insurer, said, “There is a general lack of education about the requirements of business associates. Few organizations are able to truly monitor or assess the business associates’ privacy and security practices.” Healthcare organizations are aware that when they contract with vendors, they must consider the possible privacy and security risks. Yet, many are not ready to pull the plug on a vendor if it is not in full compliance.

Also, some healthcare organizations have found that vendors are overburdened with having to respond to requests to assess their privacy and security practices and don’t have

Figure 10: How healthcare organizations are ensuring business associates can be trusted with PHI.

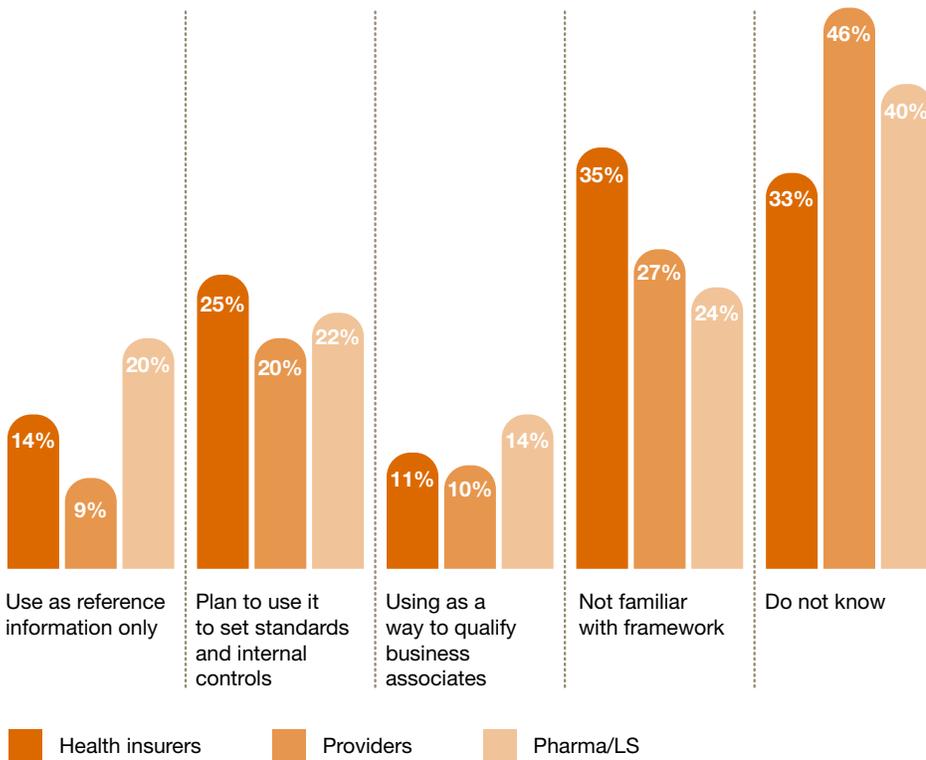
How do you ensure that a business associate (partner/vendor) can be trusted with protected health information? Please select all that apply.



Source: PwC Health Research Institute Privacy and Security Survey, 2011

Figure 11: HITRUST alliance privacy/security framework.

**What uses do you have for the HITRUST alliance privacy/security framework?
Please select all that apply.**



Source: PwC Health Research Institute Privacy and Security Survey, 2011

the staffing to support them. Others have found that the health industry’s expanding boundaries are bringing in vendors and business partners with little knowledge of what kind of privacy and security requirements and restrictions they’re up against. (For more information on new entrants to the health industry, see *The new gold rush: Prospectors are hoping to mine opportunities from the health industry*).

Thomas Jefferson University Hospital has placed a significant focus on this issue by dedicating a team to review business associate agreements that have been in place over the past year. “Privacy and security efforts have become extremely time consuming because everyone wants to be 100% certain they are in compliance,” said Thomas J. Lewis, president and chief executive officer. “It’s hard to balance

the risk mitigation level with the resources that are available. If you want to have a culture of safety and privacy, it’s hard to tell your employees not to look at every single detail and ask instead that they reach a confidence level about our compliance based on the review of key metrics and/or areas of major concern.”

One issue for healthcare organizations is that 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 that organizations that create, access, store, or exchange personal health and financial information can use.

Although organizations are increasingly considering requiring their business associates to become HITRUST certified, only 7% of PwC survey respondents said they do so yet, and only 10% said their business associates are already HITRUST certified or will be in the next six months. (See Figure 11).

The trend in the pharmaceutical and life sciences sector over the last few years has been to outsource IT functions to third parties for cost savings and to better deliver capabilities globally, but only 17% of survey respondents from the sector said that they have addressed the privacy and security issues related to Internet-based outsourced IT functions like cloud computing. The trend toward cloud computing will continue—and extend to health insurers and providers—as healthcare organizations try to

Figure 12: Privacy and security challenges for secondary data use.

Regarding your secondary use of data, please identify your top 3 challenges.



Source: PwC Health Research Institute Privacy and Security Survey, 2011

manage growing IT infrastructure and costs. Some IT vendors may already be outsourcing their storage duties to cloud vendors without healthcare organizations even knowing. With cloud options popping up everywhere, organizations need to be mindful of how these options are selected and managed from a privacy and security perspective and in what countries and under what laws their IT vendors might be pushing functions to the cloud.

3. Secondary data use

Nearly three-quarters of healthcare organizations are using it despite privacy concerns.

In a recent PwC survey, although only 20% of respondents said they have had problems with privacy as it relates

to secondary data use, over 80% of respondents cited privacy, legal implications, and public relations ramifications as concerns.¹² But, according to our survey, of those that said they are using secondary data, less than half have addressed or are in the process of addressing privacy and security. (See Figure 12).

Top challenges for the industry related to using secondary data were establishing information security functions, appropriately encrypting data, and creating multiple levels of separation between the data and the end consumer. Health insurer respondents were more concerned (40%) than providers (33%) and pharma/life science companies (22%) about de-identifying data. HIPAA defines

18 data elements that must be removed for data to be considered de-identified. Healthcare organizations need to make sure they are adhering to these rules if they intend to expand their uses of data. Many healthcare organizations are looking for effective statistical de-identification solutions to use data for data analytics and other secondary purposes.

In addition, the possibilities for using secondary data grow as organizations understand more about what affects health status. “I think the definition of health data is expanding in this environment,” said Kevin Haynes, information

¹² Transforming healthcare through secondary use of health data, PricewaterhouseCoopers Health Research Institute, 2009.

Outcomes research requires a convergence of health data cloaked in privacy

HealthCore, Inc. is moving outcomes research and informatics forward by getting providers, health plans, and pharmaceutical companies to share data to reach a common goal. Critical to gaining and maintaining data sharing partners, though, is the ability to build credibility with providers around data privacy and security. “In the past, much of our research where we utilized clinical data from the chart was done on a project-by-project basis,” said Marcus Wilson, the company’s president. “Now we are building an approach to privacy and security that will position us to expand our research by leveraging our existing data sources and integrating additional clinical sources.”

HealthCore, a Wilmington-based subsidiary of health insurer WellPoint, is partnering with AstraZeneca Pharmaceuticals to analyze the effectiveness of current medicines and treatments and provide insight into the types of new therapies. HealthCore understands clearly that administrative data alone provides only a limited view of the patient. To date, HealthCore has relied on claims data and manual extraction of data from paper-based charts for analyses that require the incorporation of clinical endpoints. While effective, this process is expensive and time consuming. Now the company will be able to create an integrated view of data by linking data elements from its claims database to providers’ electronic health records.

To create a privacy-secure foundation, HealthCore will have a separate business associate agreement with each provider, starting with an understanding that clinical data will be not be shared with WellPoint outside of any agreements between WellPoint and the provider. While WellPoint’s claims data flows to HealthCore’s database, there is no bi-directional interface that allows data to flow back to WellPoint unless permitted under these separate

agreements. Rather than manually extracting data from medical records, HealthCore will be able to interface with disparate provider EHRs.

“Privacy is something you can’t just check off and be done with; you have to actively participate in it because it is constantly evolving,” said Wilson. “This means having a proactive approach. We look at existing privacy regulations, but we challenge ourselves to go a step further and act in the spirit of the regulations and their intended purpose when developing our internal policies.”

At the end of the day, HealthCore keeps the value to the patient top of mind. “Many of our organization’s leaders are clinicians by background,” said Wilson, who is a clinical pharmacist. “There’s something to be said about having interacted with patients as caregivers ourselves. We have a good understanding of how the patient would feel about how their data is being used and always keep this in mind when using their data.”

security officer at Nemours. “I compare this to how we now refer to the electronic medical record as the electronic *health* record and *clinical* informatics as health informatics. Also, ‘*medical* and *wellness*’ don’t relate to each other as much now as do ‘*health* and *wellness*.’”

Yet, this expansion can blur the definition of protected health data. “If organizations are linking any health-related data to PHI, I don’t see why they should treat these data any differently than the PHI itself,” said Marcus Wilson, president of HealthCore, Inc., an outcomes research and informatics company and subsidiary of WellPoint, the nation’s largest health insurer. “The same protections should be in place to ensure the integrity of the data and protect the patient’s privacy.” (See Sidebar: *Outcomes research requires a convergence of health data cloaked in privacy*).

There is evidence the federal government is becoming increasingly involved in deciding the permitted uses of health data. For example, in June 2011, the Supreme Court struck down a Vermont law that prohibited the marketing of pharmaceuticals to doctors based on prescription information gathered by data miners.¹³ Many medical professionals viewed the decision as

controversial, arguing that physician prescribing patterns are private information and that the sale of prescription information for marketing purposes does not directly improve the health-care industry or the quality of patient care. The Supreme Court decided otherwise: the use of this information will be regarded as free commercial speech. The industry might expect further debate to ensue as the federal government and other regulatory bodies becomes more interested in the permitted uses of secondary health data.

Patients are also becoming more interested in sharing their data to benefit themselves and others. For example, 69% of patients would consider allowing their experience with prescription medications and health data to be included in a global research database to assist in the discovery of new medicines.¹⁴ Also, more than 100,000 patients have joined Patientslikeme.com, a social networking site that virtually connects patients with similar conditions to share their health experiences and provide a forum for patients to learn from one another.¹⁵ Patients participate with the understanding that much of the information they provide is for public consumption. But patients need to know how their data is being used

Pharmaceutical/life science companies were more likely than providers and health insurers to report social media as a top privacy/security concern.

13 Modern Healthcare, Supreme Court strikes down Vt. data-mining regulation, June 23, 2011, accessed June 28, 2011, <http://www.modernhealthcare.com/article/20110623/S/306239962?AllowView= VW8xUmo5Q21TcWJOb1gzb0tNN3RLZ0h0MWg5SVgra3NZRzRO R3l0WWRMZmJVdjhDRWxiNUtpQzMyWmV0NVg4WUpicWo=>.

14 Quintiles, The New Health Report 2011, accessed June 13, 2011, <http://www.quintiles.com/elements/media/files/2011-new-health-report.pdf>.

15 Patientslikeme, accessed June 28, 2011, <http://www.patientslikeme.com>.

Organizations should learn to manage this tool and maximize the benefits it offers, rather than just blocking access.

and have confidence that it is being aggregated appropriately. “This is not rocket science—organizations need to engage the patient community from the start in order to succeed,” said Margaret Anderson, executive director of FasterCures, an organization focused on facilitating cross-sector collaborations needed to accelerate research and development. “The organizations we see succeed over and over again view the patient as a key stakeholder and allow them to help tailor the model for secondary data use.”

Educating patients, fully disclosing the intended uses for their data, and providing the option to opt out will be critical to advancing care through informatics. Healthcare organizations must also establish controls over how much data is collected for secondary uses—“minimum necessary”—and the access of this data to protect the patients’ privacy.

4. Virtual touchpoints

Social media: Less than 40% of organizations surveyed said they have included social media in company privacy trainings.

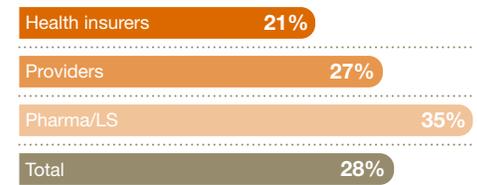
At Thomas Jefferson University Hospitals in Philadelphia, enterprising hospital department and program directors are eager to set up Facebook pages. “The cancer center wants one, the surgery department has one, and what we’re focusing on now is how to manage the creation and content of these sites so that they can be

used appropriately and as effective marketing tools that provide accurate information to our patients and the general public,” said Monica Doyle, senior director for marketing research, strategy, and consumer Internet.

Only 28% of survey respondents indicated social media as a top privacy and security concern, but this may be attributable to how lightly healthcare organizations seem to be treading as a result of privacy and security regulations having not caught up to the proliferation in social media use. (See Figure 13). In fact, interviews with healthcare executives told another story. Most acknowledged their awareness that patients are demanding that organizations be visible on the Internet and accessible in social media channels, but cited several prevailing concerns.

Figure 13: Level of privacy/security concern related to social media.

Social media is one of my top three privacy/security concerns.



Source: PwC Health Research Institute Privacy and Security Survey, 2011

Organizations appear most concerned with five user groups: (1) employees using social media for personal use, (2) employees using social media for business purposes, (3) consumers and patients seeking information and online interactions, (4) competitors, and (5) advocacy groups. All user groups have the potential to threaten the reputation of an organization.

Employee access to social media varies among organizations. Although some organizations have embraced social media channels, others have banned access completely or have provided limited use by blocking personal use. “All social media is, is a new form of communication—like the phone and email was at one point. Organizations should learn to manage this tool and maximize the benefits it offers, rather than just blocking access,” said the Society of Corporate Compliance and Ethics and Health Care Compliance Association’s Snell.

“We’ve decided that to retain staff and be an employer of choice, it’s going to be critical for us to provide at least some level of access to social media,” said Nadia Fahim-Koster, director of information security and compliance at Piedmont Healthcare. While 54% of healthcare organizations say they allow access to at least one social networking site while at work, less than half have a policy covering the use of social media outside of work.¹⁶ Only 37% of organizations surveyed noted that they have included social media in company privacy training.

In order to be successful in addressing social media challenges, organizations must establish policies and communicate these in conjunction with privacy trainings. In addition, resources must be dedicated to monitoring the content posted on social media to ensure the appropriateness of the content in all posts and/or feedback posted. The reaction level may be limited, however. For example, as health insurers plan to enter the health insurance exchanges in 2014, there is a privacy concern that limits health insurers’ ability to fully respond to negative feedback. It’s nearly impossible for health insurers to publicly respond to inaccurate statements about a member’s experience because they aren’t able to disclose the conversations related to the member’s health or healthcare. (For more information on health insurance exchanges, see *Change the channel: Health insurance exchanges expand choice and competition*).

Pharmaceutical/life science companies were more likely than providers and health insurers to report social media as a top privacy/security concern (35% compared to 27% and 21%, respectively). But approximately 23% of pharmaceutical organizations said they have not begun to address the privacy and security implications of social media. A key objective among pharmaceutical companies is to come

as close as possible to achieving direct contact with the consumer, but the US Food and Drug Administration is very stringent about product placement on social media and has yet to develop guidelines for its use. Many pharmaceutical companies therefore have been utilizing social media as a broad-based informational tool only.

Others have found a different strategy that they believe brings them more value and a lower level of risk. “The best way for pharmaceutical companies to get in on the social media space is to partner with an online community,” said Julie Kudyba, global privacy officer at Novartis Pharma AG. Partnering with such organizations offers pharmaceutical companies sponsorship opportunities, access to aggregated data analysis, and the potential to conduct closed sessions with patients upon invitation.

16 The Society of Corporate Compliance and Ethics and the Health Care Compliance Association, Social Media Survey, 2011.

Approximately 1,200 providers have ventured into social networking platforms.¹⁷ Soon, though, patients may be turning to their providers to help them connect with other patients facing similar health issues. “I believe patients are increasingly going to be looking beyond national online patient forums where they can interact with people that are having a local experience,” said Hartford HealthCare’s Taveras. “Having providers duplicate national or global online patient connectivity forums can only help patients who want to know what others are experiencing within their own communities.” Providing a forum that promotes open communication and benefits the community by enabling people to share information could be considered a differentiator by consumers as long as privacy and security issues are addressed.

Mobile devices: Less than half of health organizations surveyed have addressed or are addressing privacy and security.

How can organizations embrace the use of mobile devices and reap the benefits they have to offer, while still protecting the privacy and security of patients and consumers? They must ensure that

policies are in place to secure devices and to limit the information stored on local drives, a particular concern with mobile. PwC defines mobile health broadly as the ability to provide and receive healthcare treatment and preventative services outside of traditional care settings. Mobile health tools can include remote patient monitors, video conferencing, online consultations, personal healthcare devices, wireless access to patient records, and prescription applications using a cell phone, smartphone, or wireless tablet. Some organizations believe that utilization of the devices can be beneficial to patient care and operational efficiency so they do not limit the type of mobile device. Rather, they provide choice with enterprise-wide standards.

Advancements in technology and increased benefits provided by supported applications have led to the explosion of mobile devices in the healthcare industry. But the broad access procedure requirements under the HIPAA minimum-necessary rule resulted in a slew of generic log-ons for mobile devices like computers on wheels, workstations on wheels, and

¹⁷ FierceHealthcare, Patients pick hospitals for their social media presence, June 29, 2011, accessed July 14, 2011, <http://www.fiercehealthcare.com/story/patients-pick-hospitals-their-social-media-presence/2011-06-29>.

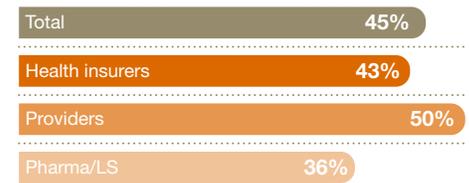
tablets that are now standard devices in the day-to-day operations of health-care organizations. According to interviews, the industry is concerned about how generic access has left their organizations vulnerable. Although these devices are enabling more efficient workflows, less than half of all survey respondents have addressed or are addressing privacy and security as it relates to mobile devices. Pharmaceutical and life sciences companies were least likely to have figured out an approach (36%). (See Figure 14). This is especially concerning, as there have been 39 health information breaches involving portable devices since 2009 and these breaches affected approximately 1.4 million individuals.¹⁸

In some cases, healthcare organizations also need to increasingly understand the security of consumer mobile devices. For example, to improve patient care and access while managing

its information technology budget, Boston Medical Center, a 508-bed academic medical center, is instituting a “bring your own device” to work policy. Healthcare professionals will have on-the-job access to some hospital systems and records on their personal mobile devices.¹⁹ Also, some pharmaceutical companies are turning to mobile devices to connect with patients and monitor such things as drug adherence. For example, Bayer introduced a product called DIDGET, a diabetes blood glucose meter that connects with a Nintendo gaming system to motivate consistent glucose testing in children. As this trend continues and patients continue to demand mobile applications, organizations will need to pay particular attention to evaluating the security of the connection, encryption, and local storage capabilities of these devices. (For more information on mobile health, see *Healthcare unwired: New business models delivering care anywhere*).

Figure 14: Privacy/security progress related to mobile devices.

Have already or are in the process of addressing a privacy/security approach to mobile devices.



Source: PwC Health Research Institute Privacy and Security Survey, 2011

¹⁸ US Department of Health and Human Services Office for Civil Rights, accessed June 27, 2011, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>.

¹⁹ MobiHealthNews, Hospitals won't ever go completely wireless, April 14, 2011, accessed July 15, 2011, <http://mobihealthnews.com/10711/hospitals-wont-ever-go-completely-wireless/>.

What this means for your business

Common strategies
for healthcare
organizations to
move forward

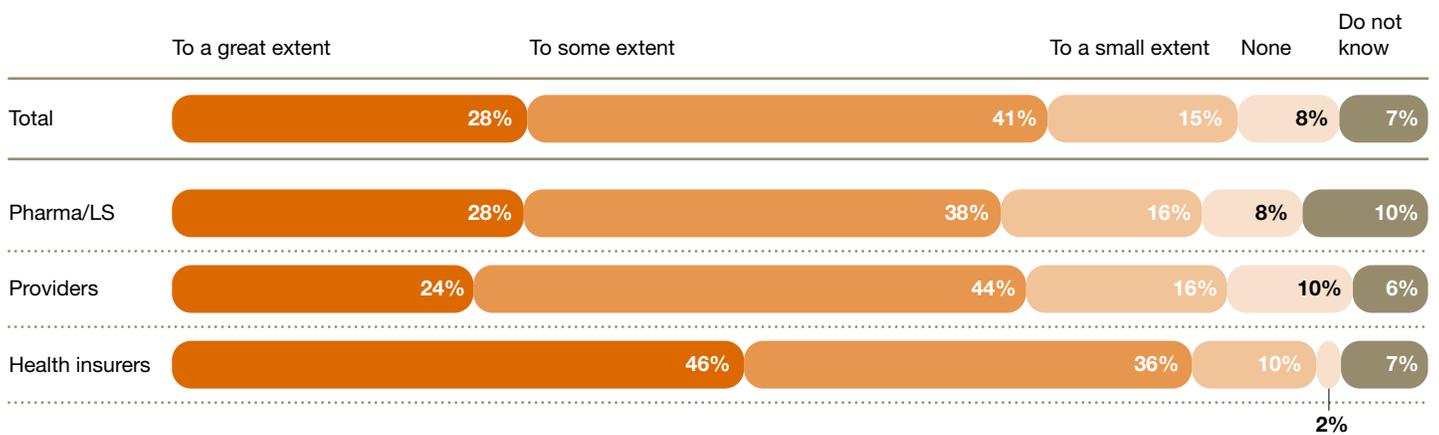
While each industry sector has its own specific privacy issues, four guidelines provide a common strategy for providers, health insurers, and pharmaceutical/life sciences firms to move forward in this environment:

- 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

Integrate privacy and security approaches

Industry-wide, 69% of healthcare organizations said they have integrated, at least to some extent, their approaches to compliance, privacy, security, and identity theft (See Figure 15). Only 28% said they have done so to a great extent, with health insurers leading the pack (46%). An integrated framework allows organizations to address regulatory requirements and address common vulnerabilities often not addressed in regulatory frameworks. The HRI survey found that organizations that have integrated approaches to a great extent have seen distinct benefits.

Figure 15: Extent to which organizations have developed integrated approaches/frameworks that combine compliance, privacy/data usage, security, and ID theft.



Source: PwC Health Research Institute Privacy and Security Survey, 2011

Figure 16: Benefits experienced by organizations that have integrated approaches/frameworks for compliance, privacy, security, and identity theft.

	Integrated approaches to a great extent	All others
The security of my organization's data has increased compared to last year.	66%	49%
Compared to last year, my organization's privacy/security staffing has increased.	48%	31%
Average reported number of privacy/security issues per respondent in last two years.	1.14	1.22

On average, as shown in Figure 16, these organizations reported being:

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

Health insurers may have heightened awareness about the organization's privacy and security since, historically, they have been subject not only to HIPAA, but also to financial regulations that motivated them to integrate approaches and frameworks earlier than the other sectors. 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). While pharmaceutical companies have been subject to multiple regulations globally, they have generally taken a fragmented privacy and security approach by country. Only in the last few years, through their Safe Harbor efforts, have they started building global approaches. Providers largely have underinvested in integrated approaches, focusing only on HIPAA compliance because they were not subject to multiple regulations, until now.

"The key is to implement an information governance strategy with an integrated compliance and operations plan," said Ken Mortensen, vice president, assistant general counsel, and chief privacy officer at CVS Caremark. "Information, including personal health records, is the most critical asset of any organization, and leadership

needs to ensure that this information is treated both appropriately and strategically.” In 2006, the retail business of CVS Caremark experienced an incident concerning PHI when items, such as pill bottles, with patient information were reportedly found in the trash, resulting in investigations by FTC and OCR. Since then, the company has focused on enhancing its strategic approach to compliance and operations surrounding the information, especially privacy protections, Mortensen said.

In addition, healthcare organizations should conduct data inventories, assess compliance, and benchmark controls. “Surfacing risks and addressing them are extremely important to our ability to deliver our mission. Therefore, we have an extensive compliance strategy,” said Tammi Keating, vice president of compliance strategy and operations at Kaiser Foundation Health Plan, Inc. “Through standard risk and compliance assessment tools, we identify where compliance risks have happened in the past, assess the likelihood of past and future risks occurring, and engage our operational leaders to align their goals and priorities with compliance risk mitigation efforts.”

Make minimum controls and standards a prerequisite to play

Minimum controls and encryption

As healthcare organizations ponder entry into new business ventures made possible through the data-sharing playground, they must decide what data to encrypt and maintain a minimum set of internal and external privacy and security controls. The decision is becoming increasingly important as new healthcare technology service providers and other third parties seek to partake in the game. Business associates, especially those inexperienced in healthcare, will likely welcome guidance on how to comply with the increasingly complex laws governing the industry and address gaps in the regulations. This gives healthcare organizations an opportunity to assume control of negotiations by having already developed specific standards that their business associates must meet.

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. “The regulations are exposed, similar to the small part of the iceberg which is above water,” said one healthcare provider executive. “But the largest part—how to comply with these regulations—hides below the surface. There are significant risks associated with not looking below the surface.”

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

Healthcare organizations need to educate and hold their employees accountable for privacy.

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.

Without a minimum set of controls and a document detailing their privacy and security programs, organizations might have a barrier to entry into new business opportunities. To make privacy and security enablers to enter these businesses, minimum controls must be specific.

Standards-based approach

Regulations and standards are similar, but not the same. 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. Taking a "compliance approach" to security is not the most effective use of resources given the potential operational and reputational risks involved with security threats. Security breaches of several prominent payment card industry-compliant companies point out that compliance does not directly translate to security.

Healthcare organizations should design their privacy and security capabilities using a flexible framework (e.g., ITIL or COBIT) to provide a controls-based foundation to work from and to help decrease rework as regulatory requirements change. Through a standards-based approach, organizations perform periodic reviews of internal controls and clearly link controls back to both current and pending regulations. Historically, some healthcare organizations' approach has been to secure everything, but this is not efficient. One healthcare executive noted, "Security is a form of life insurance, but how much do we need to buy? With a standards-based approach, organizations can actually spend less on security because they know where to focus." By not evaluating the regulations and standards, organizations run the risk of developing policies and frameworks with gaps. If these gaps are significant and a data breach occurs, regulators might argue that the organization did not have reasonable controls in place.

Deputize all workers as privacy champions

Healthcare organizations need to educate and hold their employees accountable for privacy. That means creating a culture of confidentiality in which everyone is responsible for privacy and receives a form of privacy awareness training. “The privacy officer should be the monitor of what’s going on in the organization, not the instigator of privacy practices,” said Thomas J. Lewis, chief executive officer at Thomas Jefferson University Hospitals. “That needs to come from the top. After the message is communicated, organizations can’t rely only on the privacy officer to manage every aspect of privacy. It is critical for middle management to be privacy oriented in order to build a culture of confidentiality.”

Privacy and security initiatives should be incorporated into each business unit, with centralized oversight. Roy Snell, of the Society of Corporate Compliance and Ethics and Health Care Compliance Association, said “There should be employees within each business unit that are responsible for integrating and maintaining privacy and security. These individuals should report to a supervisor that is looking at the privacy and security culture from a centralized, high level.”

For example, in the offices of some of its large physician group practices, CIGNA has placed case managers and coaches who meet with patients prior to their appointment to discuss care plans. These individuals are able to double as privacy champions.

Healthcare organizations need to make sure that employees and physicians have the training to make good decisions regarding the protection of patient data, but not make them afraid to do their jobs. According to interviews, some employees are beginning to shy away from accessing personal health information even when it would be appropriate to do so. “When we conduct privacy trainings with our physicians, we make it clear that regulations should not be a barrier to doing what’s right for our patients—patient safety and treatment come first,” said Sam Strally, privacy officer at Nemours. Providers and health insurers need to increase their focus on EHR training—only 58% of providers and 41% of health insurers reported including appropriate EHR use as a component of their privacy training for employees.

Organizations have opportunities to address misconceptions related to privacy and security laws. “Organizations really need to proactively manage privacy and compliance because one of the unforeseen consequences of regulations is misinformation and misinterpretation,” said one executive from a large pharmaceutical company. “There are many misconceptions in the provider environment among clinical investigators about what is permitted. They are quick to say: ‘We can’t do that,’ when they are actually missing opportunities.”

Some employees are beginning to shy away from accessing personal health information even when it would be appropriate to do so.

An organization can start to build a culture around confidentiality, beginning with raising the level of awareness and appropriate behavior. For example, one academic medical center representative said that while it encrypts emails found to contain PHI within the hospital, the affiliated university practice plan does not. Physicians are now putting pressure on the university to increase security as they are now more knowledgeable about the risks of transferring data. It annoyed them that when they send information from their university accounts, it isn't encrypted.

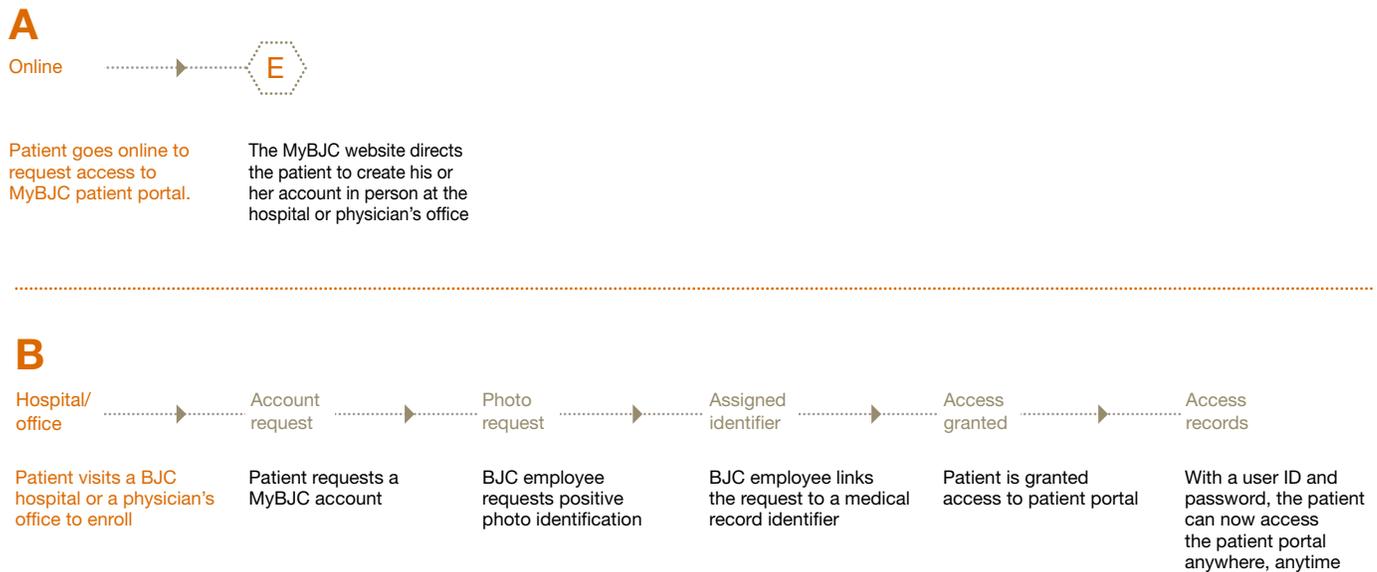
Healthcare organizations can also help privacy and security professionals understand how their roles impact operations. "My goal is to enable clinicians to be more efficient while maintaining security of data," said Kevin Haynes of Nemours. "I aim to balance confidentiality, integrity, and availability by continually asking myself, 'How can I do what I need to do from a security perspective without hampering the care model and clinicians' workflows?'"

Some organizations are more heavily involving the chief privacy officer in proactive business discussions. "HIPAA taught us to be reactive, but today our organization operates in a much more proactive mode," said Lisa Martinelli, chief privacy officer at Highmark Inc., an independent licensee of the Blue Cross and Blue Shield Association that serves Pennsylvania and West Virginia. "The privacy office is involved with strategic development of new products and services and regarded as a collaborative business partner. My role is to get into the business decisions when they are being created. We find this reduces the need for me to say 'no' to initiatives on the back-end because I've been involved in their development and have spotted and addressed privacy issues in advance."

Make privacy part of the consumer experience and brand

There's a disconnect between patients and the healthcare industry about how personal health data is used, but patients are likely to start connecting the dots soon as they learn about health reform, whether through ACOs, HIEs, or health insurance exchanges that are currently under development, and the importance of data sharing in all of these.

Figure 17: BJC HealthCare: Educating patients about privacy and security through patient portal.



“An organization’s approach to privacy should be something that is marketed in conjunction with the services that it offers,” said Hope Scott, senior privacy counsel at CIGNA. “We rely on our salespeople to connect with the group market regarding privacy through our partnerships with brokers and consultants. With an expansion in the individual market from the pending health insurance exchanges, our approach to privacy needs to be through multiple points of engagement with the consumer. It can’t just be through paper anymore.”

Healthcare organizations will benefit from connecting with patients and consumers about the importance of privacy within the context of the value of their health data in advancing care and improving the healthcare delivery

system. “One of our board members recently asked us how compliance fits into our strategy,” said Henry Neidermeier, vice president–information technology compliance at Kaiser Foundation Health Plan, Inc. “I believe compliance becomes the strategy behind developing and maintaining a trusted brand.”

At BJC HealthCare in St. Louis, privacy was of paramount importance in development of its patient portal, myBJC.org, that allows patients to view test results and communicate with physicians online, as well as get access to other health information. The organization has a single source of access to register for an account requiring face-to-face contact. (See Figure 17). “To safeguard patient privacy, patients can access information about MyBJC online, but enrollment can only be

done in the physician’s office or in the hospital with positive photo identification. Our staff then links that request to a medical record identifier,” said David Weiss, BJC’s senior vice president and chief information officer. “You would think that marketing would have fought this because it does add hurdles to the patient sign-up process, but they are actually completely on board with this added level of security and defend it. I think they realize that this is another way for us to differentiate our patient portal offering because we are taking the time to demonstrate to patients that their privacy is as important to us as it is to them.”

This report is the fourth in a series of reports on the IT implications of health reform and other regulatory requirements. The research for this report included 25 in-depth interviews with thought leaders and executives in the health industry, including hospital providers, health insurers, pharmaceutical/life science companies, and advocacy groups. HRI also commissioned in spring 2011 an online survey of approximately 350 provider executives, 100 health insurer executives, and 180 pharmaceutical/life sciences executives in privacy, compliance, information technology, and operations.

About PwC

PwC firms provide industry-focused assurance, tax and advisory services to enhance value for their clients. More than 161,000 people in over 150 countries in firms across the PwC network share their thinking, experience, and solutions to develop fresh perspectives and practical advice. See www.pwc.com for more information.

Health Research Institute

PwC's Health Research Institute provides new intelligence, perspectives, and analysis on trends affecting all health-related industries. The Health Research Institute helps executive decision makers navigate change through primary research and collaborative exchange. Our views are shaped by a network of professionals with executive and day-to-day experience in the health industry. HRI research is independent and not sponsored by businesses, government, or other institutions.

PwC Health Research Institute

Kelly Barnes
Partner, Health Industries Leader
kelly.a.barnes@us.pwc.com
(214) 754-5172

Serena Foong
Senior Manager
serena.h.foong@us.pwc.com
(617) 530-6209

David Chin, MD
Principal (retired)
david.chin@us.pwc.com
(617) 530-4381

Sarah Haflett
Manager, Health Information
Technology Research
sarah.e.haflett@us.pwc.com
(267) 330-1654

Sandy Lutz
Managing Director
sandy.lutz@us.pwc.com
(214) 754-5434

Meredith Wasko
Research Analyst
meredith.l.wasko@us.pwc.com
(617) 530-4632

Benjamin Isgur
Director
benjamin.isgur@us.pwc.com
(214) 754-5091

Health Research Institute Advisory Team

James Koenig
Director and Co-leader
Health Information Privacy and
Security Practice
james.h.koenig@us.pwc.com
(267) 330-1537

Emmanuelle Galland
Director
emmanuelle.galland@us.pwc.com
(646) 471-7123

Agatha O'Malley
Manager
agatha.l.omalley@us.pwc.com
(267) 330-1834

Preetham Peter
Director
preetham.s.peter@us.pwc.com
(415) 498-7162

Rik Boren
Partner
rik.boren@us.pwc.com
(314) 206-8899

TR Kane
Principal
t.kane@us.pwc.com
(216) 875-3038

Robin Settle
Director
robin.m.settle@us.pwc.com
(267) 330-4006

Health Industries Marketing

Todd Hall
Director
todd.w.hall@us.pwc.com
(617) 530-4185

Attila Karacsony
Director
attila.karacsony@us.pwc.com
(973) 236-5640

Nadia Leather
Director
nadia.m.leather@us.pwc.com
(646) 471-7536

Hindy Shaman
Director
hindy.shaman@us.pwc.com
(703) 453-6161

Acknowledgments

Margaret Andersen
Executive Director
FasterCures

Jennings Aske
Chief Information Security Officer
Partners HealthCare

Debra Bromson
Senior Counsel,
Commercial and Privacy
AstraZeneca Pharmaceuticals

Dan Colin
Director of Global Security and
Privacy Officer
Hospira

Greg Dinklenburg
Manager, Global Information
Governance and Privacy Hospira

Monica Doyle
Senior Director for
Marketing Research, Strategy, and
Consumer Internet
Thomas Jefferson University Hospitals

Acknowledgments, continued

Nadia Fahim-Koster
Director, Information Security and
Compliance
Piedmont HealthCare, Inc.

Kimberly S. Gray, Esq., CIPP
Chief Privacy Officer, Global
IMS Health

Kevin Haynes
Information Security Officer
Nemours

Tammi Keating
Vice President, Compliance Strategy
and Operations
Kaiser Foundation Health Plan, Inc.

Kirk Koehler
Senior Project Manager, Privacy
Wal-Mart

Julie Kudyba
Global Privacy Officer
Novartis Pharma AG

Thomas J. Lewis
President and Chief Executive Officer
Thomas Jefferson University
Hospitals, Inc.

Lisa Martinelli
Chief Privacy Officer
Highmark

Kenneth Mortensen
Vice President, Assistant General
Counsel and Chief Privacy Officer
CVS Caremark

Henry Neidermeier
Vice President —Information
Technology Compliance
Kaiser Foundation Health Plan, Inc.

Hope Scott
Senior Privacy Counsel
CIGNA

Brian Selfridge
Chief Information Security Officer
AtlantiCare

Roy Snell
Chief Executive Officer and
Co-Founder
Society of Corporate Compliance and
Ethics and Health Care Compliance
Association

Janet Steiner, RN
Senior Director, R&D Health
Care Compliance
Shire Pharmaceuticals

Sam Strally
Privacy Officer
Nemours

Luis Taveras
Senior Vice President of Information
Technology Services
Hartford HealthCare Corp.

Marcus Wilson
President
HealthCore, Inc.

External Health IT Thought Leadership Advisory Group

Pamela McNutt
Senior Vice President and Chief
Information Officer
Methodist Health System

Mark Pasquale
Chief Information Officer
Piedmont HealthCare

William Robinson
Chief Financial Officer
Shands HealthCare

David Weiss
Senior Vice President and Chief
Information Officer
BJC HealthCare

pwc.com/us/healthindustries
pwc.com/hri
twitter.com/PwCHealth

***To have a deeper conversation
about how this subject may affect
your business, please contact:***

Daniel Garrett
Principal and National Leader
Health Information Technology
PwC
daniel.garrett@us.pwc.com
(267) 330-8202
Philadelphia

James Koenig
Director and Co-leader
Health Information Privacy and Security Practice
PwC
james.h.koenig@us.pwc.com
(267) 330-1537
Philadelphia

Peter Harries
Principal
Co-leader
Health Information Privacy and Security Practice
PwC
peter.harries@us.pwc.com
(213) 356-6760
Los Angeles