

## Issue Brief:

# Privacy and Security in Health Care: *A fresh look*

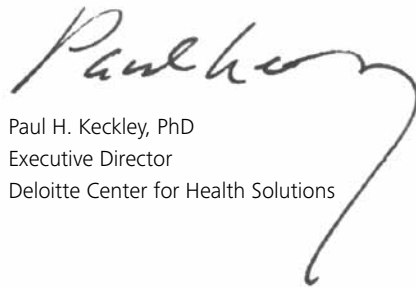
### Foreword

The United States health care industry is data-rich. Every encounter with the system results in an electronic footprint. The promises of connectivity – electronic and personal health records, clinical warehousing, home monitoring, distance medicine, and more – mean exponential increases in data and, in tandem, exponential opportunities for breaches of privacy and security of personal health information.

Facebook Co-Founder Mark Zuckerberg is a household name because his trade – connectivity, information, data flow – and “data” has ubiquitous impact on daily lives. Health care information is no less ubiquitous.

This Issue Brief provides a primer on risks associated with privacy and security in health care and guidance about industry preparedness.

Privacy and security is a significant challenge for every health care organization and a concern for every U.S. citizen.



Paul H. Keckley, PhD  
Executive Director  
Deloitte Center for Health Solutions

### Background

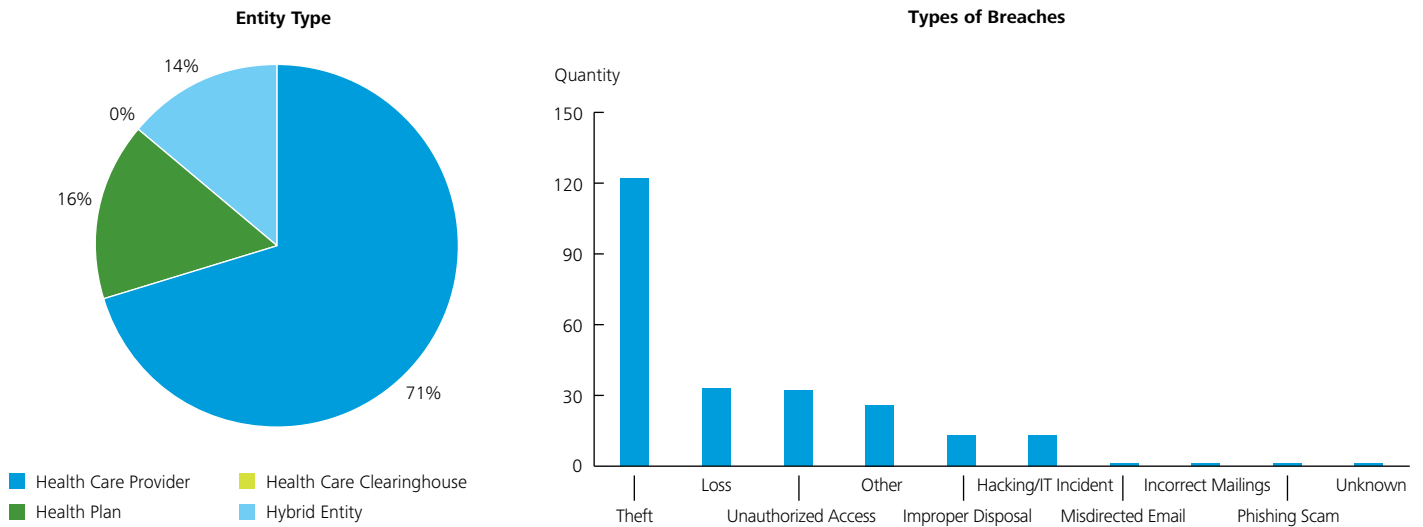
On September 20, 2010, a computer flash drive containing the names, addresses, social security numbers (SSNs), and protected health information (PHI) of 280,000 Medicaid members was stolen from the corporate offices of a health plan.<sup>1</sup> On May 3, 2006, a laptop and disc containing personal health information (names, SSNs, date of birth, and other information) for 26.5 million veterans was stolen from a Veterans Administration (VA) employee's home.<sup>2</sup> Personal health information about Congresswoman Nydia Velasquez, country singer Tammy Wynette,<sup>2</sup> and “octomom” Nadya Suleman were accessed, resulting in civil fines<sup>3</sup> and embarrassment to reputable health systems.



In the seven years following the enactment of the Health Insurance Portability and Accountability Act (HIPAA) in April 2003, the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) has investigated and resolved over 11,000 HIPAA violations.<sup>4</sup> Since enactment

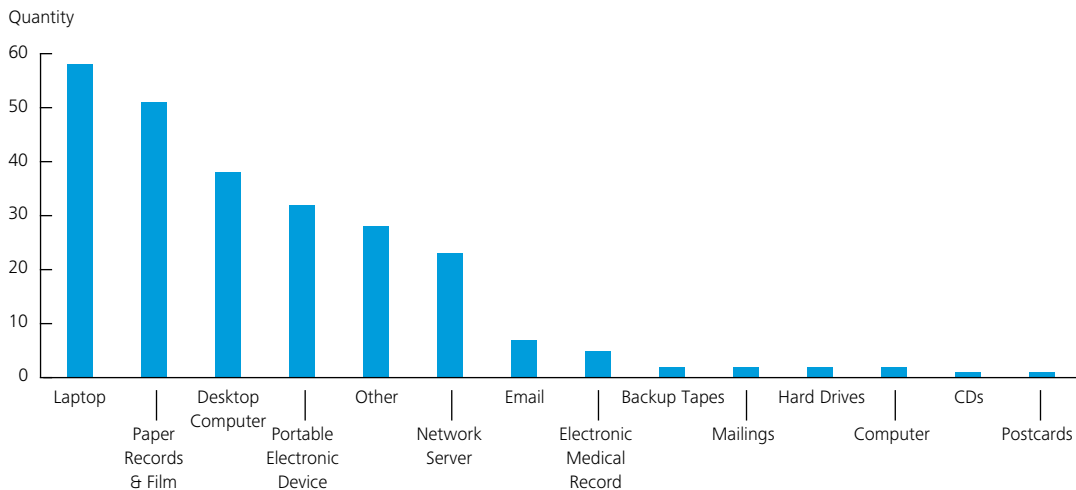
of the Interim Final Breach Notification Rule in September 2009, nearly seven million patients have been affected by data breaches.<sup>5</sup> Figure 1 depicts some key statistics about breaches reported by HHS.

**Figure 1: HHS-reported information breaches**



Note: Percentages may not add up to 100% due to rounding.

**Location of Breached Information**



Based on data published by HHS as of December 27, 2010

© 2011 Deloitte Development LLC. All rights reserved.

As used in this document, "Deloitte" means Deloitte & Touche LLP and Deloitte Consulting LLP, which are subsidiaries of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

The health care industry is particularly susceptible to data fraud and medical identity theft due to the nature and content of the data it creates, collects, and stores.<sup>6</sup> Sensitive data such as SSNs, insurance identification numbers, payment information, and medical provider identification numbers enables criminals to file fraudulent claims that often go undetected for long periods of time.<sup>7</sup> In 2009, 66 percent of all data breaches occurred at health care organizations.<sup>8</sup> The increase in data breaches has been attributed to gaps in federal privacy regulations;<sup>9,10</sup> lack of enforcement of existing legislation;<sup>11</sup> increased automation;<sup>12</sup> pervasiveness of social media;<sup>13,14</sup> curiosity;<sup>15</sup> and the potential for widespread monetization of personal health information<sup>16</sup> by unauthorized users. The organizational consequences of data breaches can be significant: monetary penalties,<sup>17</sup> damage to reputation, and lost revenues are most notable. The total annual economic impact of data breaches on U.S. hospitals alone is \$6 billion.<sup>18</sup> Yet most health care organizations have little or no protection in place to prevent, monitor, or remedy data breaches<sup>19</sup> and funds to implement privacy and security safeguards are minimal to non-existent in operating budgets.<sup>20,21</sup> These costs are likely to increase as a result due to the fragmentation of the U.S. wherein common privacy and security policies, procedures, and processes across sectors are problematic.<sup>22,23</sup>

The total economic burden created by data breaches in the health care industry is nearly \$6 billion annually. The impact of a data breach over a two-year period is approximately \$2 million per organization and the lifetime value of a lost patient is \$107,580.

Source: <http://www2.idexperts.com/press/healthcare-news/new-ponemon-institute-study-finds-data-breaches-cost-hospitals-6-billion/>

The move toward an entirely automated health care system featuring electronic and personal health records (EHRs and PHRs), clinical data warehousing, and increased transparency means more data is at risk and suggests an urgent review of privacy and security policies and procedures.<sup>24,25</sup> This Issue Brief provides an update about current and emergent privacy and security challenges in health care, as well as preparedness measures to avoid risk.



## Glossary

Acronym/Term	Definition
HIPAA	Health Insurance Portability and Accountability Act
Privacy <sup>26</sup>	Individual ownership and control over personal health information
Security <sup>27</sup>	Protection of personal health information from unauthorized access
Covered entity (CE) <sup>28</sup>	A health care provider that conducts certain transactions in electronic form; a health care clearinghouse, or a health plan
Business Associate (BA) <sup>29</sup>	Anyone who performs on the behalf of a covered entity and is involved in the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity
PPACA	Patient Protection and Affordable Care Act
ARRA	American Recovery and Reinvestment Act
CMS	Centers for Medicare and Medicaid Services
EHR	Electronic Health Record
PHR	Personal Health Record
PHI	Personal Health Information
HIE	Health Information Exchange
HIT	Health Information Technology
HHS	U.S. Department of Health and Human Services
ONC	U.S. Office of the National Coordinator of Health Information Technology
OCR	U.S. Office of Civil Rights
CPO	Chief Privacy Officer
CFO	Chief Financial Officer
CCO	Chief Compliance Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
AHA	American Hospital Association
AMA	American Medical Association
AAMC	Association of American Medical Colleges
HIMSS	Healthcare Information and Management Systems Society
MGMA	Medical Group Management Association
LSO	Life Science Organization
RHIO	Regional Health Information Organization

### Privacy and security: hot spots

Increased use of automated technologies (i.e., e-prescribing, billing, medical claims processing, EHRs, and PHRs)<sup>30</sup> and gravitation toward local and national health information exchanges (HIEs)<sup>31</sup> have expanded the health care privacy and security landscape. Electronic exchange of patient information offers greater convenience and efficiency in health care delivery, but not without greater data risk and liability<sup>32,33</sup> due to broader access. For example, patient information exchanged via PHRs, social media networks (i.e., Facebook, Twitter), and mobile devices is subject to HIPAA regulations.<sup>34,35,36</sup> To optimize the utility of health information technology (HIT), effective exchange of data between sectors (i.e., provider groups, diagnostic laboratories, health plans, public health agencies, financial institutions, etc.) is essential.<sup>37</sup> This broader exchange, however, further distributes privacy and security risks and increases the likelihood of data breaches.<sup>38,39,40</sup>

Some notable hot spots where current policies, rules, and regulations are a focus of industry risk include:

**Business associates vs. covered entities:** Gaps in existing legislation have enabled data breaches.<sup>41,42</sup> Under HIPAA's Administrative Simplification provisions, HHS issued Privacy and Security Rules (2003) to provide guidance for protecting PHI.<sup>43</sup> The Rules defined the "technical and non-technical safeguards" that covered entities (CEs) should implement during the handling and transference of electronic protected health information (ePHI).<sup>44,45</sup> The provisions did not extend to business associates (BAs) of CEs or to the individuals within a CE, thereby interrupting the secure exchange of PHI.<sup>46</sup> BAs of CEs were only required to contractually agree to handle PHI securely while conducting business for or on behalf of a CE. In the event of a data breach, HIPAA violations only applied to CEs, not BAs, and HHS had no enforcement over them.<sup>47,48,49</sup> Additionally, penalties for HIPAA violations applied to CEs but not the individual(s) at the CE responsible for the breach, creating a gap in accountability. Loose enforcement through infrequent audits by HHS<sup>50</sup> allowed CEs and BAs to become complacent<sup>51</sup> about managing the privacy and security of PHI, thereby increasing the risk of a breach.

**Identity theft:** In health care, approximately one third of data breaches result in medical identity theft.<sup>52</sup> In August 2009, the Federal Trade Commission (FTC) began enforcing the "Red Flags Rule" to prevent identity theft. Like HIPAA, the Red Flags Rule protects sensitive information and includes credit card and social security numbers and insurance claim information. Organizations functioning as "creditors" or which have "covered accounts" are required to implement written procedures to detect, prevent, and mitigate identity theft.<sup>53</sup> Thus far, health care industry compliance with this regulation has been low, due to lack of awareness of the rules and uncertainty as to whom the rules apply.<sup>54,55</sup> According to the FTC, providers are considered "creditors" when they defer payments for services rendered until insurance payments are made.<sup>56,57</sup> Additionally, any organization that sets up a consumer account where multiple payments can be made meets the definition of a "covered account" and is also subject to the rules.<sup>58</sup> Health care organizations needed to have adequate policies and procedures in place by December 31, 2010, or be fined up to \$2,500 per knowing violation.<sup>59</sup> On December 7, 2010, Congress exempted health care providers from the Red Flags Rule.<sup>60</sup>



**ARRA timeline:** The American Recovery and Reinvestment Act (ARRA), signed into law February 17, 2009, included provisions under the Health Information Technology for Economic and Clinical Health (HITECH) Act that strengthen HIPAA enforcement and ensure that privacy and security safeguards are coupled with increased automation.<sup>61,62</sup> (See Figure 2 for HITECH effective dates.) Most importantly, the ARRA provisions extend accountability for data privacy and security to the BAs.<sup>63</sup> It also established substantially higher fines for HIPAA violations (Figure 3),<sup>64,65</sup> many of which have already been brought to the courts.<sup>66,67</sup> Specifically, under ARRA:<sup>68,69,70</sup>

- BAs (including regional health information organizations [RHIOs], HIEs, e-prescribing gateways, and software vendors) can be held accountable for HIPAA violations to the same extent as a CE.
- Individuals, as well as CEs, can face criminal penalties for HIPAA violations.
- HHS is required to investigate HIPAA violations due to “willful neglect.”
- HHS must conduct periodic audits to ensure compliance with the law, although to date, it is not clear how this will be accomplished.
- Individuals may request an account of disclosures of their ePHI.
- Individuals must explicitly authorize the transfer or use of PHI to other entities or individuals; and CEs (or BAs) must comply with patient requests for non-disclosure of procedures paid out-of-pocket to insurers.
- State attorneys general can bring civil action in federal court for HIPAA violations.
- CEs must notify individuals, HHS, and the media of a breach of unsecured PHI affecting more than 500 individuals within 60 days of knowledge of the breach; BAs of CEs must notify CEs of a data breach within 60 days of knowledge.
- To qualify for financial incentives, CEs and BAs must meet HIPAA requirements to become “Meaningful Use” certified.

**Figure 2: HITECH Act effective dates**<sup>71,72</sup>

HITECH Provision	Effective Dates
Violations subject to tiered civil money penalties; state attorney general has authority to enforce HIPAA	February 17, 2009
Interim Final Breach Notification Rules effective	September 2009
HHS to publish guidance on technologies and methodologies that render PHI “unusable, unreadable, or indecipherable;” also, regulations on scope of BA requirements	February 2010
HHS to publish guidance about use of information	August 2010
CMS EHR incentive payments begin for hospitals	October 2010
CMS EHR incentive payments begin for eligible providers	January 2011

**Figure 3: New HIPAA violation penalty tiers under HITECH**<sup>73</sup>

Tiers	Per Violation	Maximum
Without knowledge/intent	\$100	\$25,000
Due to reasonable cause	\$1,000	\$100,000
Willful neglect	\$10,000	\$250,000
Willful neglect, not corrected	\$50,000	\$1,500,000

## Current state of preparedness for privacy and security risk

Health care industry studies suggest that current preparedness for privacy and security risk is woefully inadequate (Figure 4). Root causes vary but include lack of internal resources (human and capital); lack of

internal control over patient information; lack of upper management support; outdated policies and procedures or non-adherence to existing ones; and inadequate personnel training – all of which contribute to the rise in data breaches and medical identity theft cases in the industry.<sup>74,75,76,77,78,79</sup>

**Figure 4: Key findings from various security studies**<sup>80,81,82,83,84,85</sup>

Study (study dates)	Sponsor	Respondents	Key Findings
Spring 2010 National Survey of Hospital Compliance Executives (March 30-April 13, 2010)	AHA; Identity Force	220 hospital executives from 43 states; included CPO, CFO, CISO, CIO, Compliance Officers, HIPAA Officers, and their director-level equivalents	<ul style="list-style-type: none"> <li>Nearly 85 percent of hospitals are NOT in compliance with the HITECH Act</li> <li>Breaches up over 120 percent – 41 percent of hospitals now have ≥ 10 data breaches annually</li> <li>Potential patient ID fraud and misuse going un-investigated as 34 percent of hospitals keep inadequate photo ID records and 70 percent investigate less than one case per week</li> <li>56 percent of hospitals expect new health care reform law to either make no difference or to actually increase medical identity theft</li> </ul>
2010 HIMSS Security Survey (September 10-October 8, 2010)	HIMSS; MGMA; Intel	272 executives from hospitals, medical practices, payors, home health agencies, military health facilities, or HIEs; included CIOs, CSOs, and 10 percent VPs of information security (IS)	<ul style="list-style-type: none"> <li>General environment's level of maturity is average (4.47 out of 7)</li> <li>53 percent have a dedicated CISO/CSO or full-time security staff</li> <li>Nearly 50 percent indicate &lt;3 percent of their IT budget is allocated for information security</li> <li>59 percent of those who conduct formal risk analyses do so annually</li> <li>33 percent of respondents have reported at least one known incident of medical identity theft at their organizations</li> <li>Compared to HIMSS 2009 Security Survey, awareness of new privacy and security provisions has increased; however, preparedness has not</li> </ul>
Benchmark Study on Patient Privacy and Data Security (June-September, 2010)	Ponemon Institute; ID Experts	211 executives from 65 provider organizations; included senior-level managers from billing, medical records management, HIPAA compliance officers, CISOs, CSOs, and CCOs	<ul style="list-style-type: none"> <li>60 percent of organizations had &gt;2 data breaches in the past two years</li> <li>Data breaches cost organizations on average \$1 million annually</li> <li>The average number of lost or stolen records per breach was 1,769</li> <li>The top three causes of a data breach are: unintentional employee action, lost or stolen computing devices, and third-party snafu</li> <li>41 percent discovered the data breach as a result of a patient complaint</li> <li>58 percent of organizations have little or no confidence that their organization has the ability to detect all patient data loss or theft</li> <li>63 percent of organizations say it took them between one to six months to resolve the incident</li> <li>Inadequate budget and lack of trained staff or end users are top two reasons for data breach</li> </ul>

continues on next page

continued from previous page

Study (study dates)	Sponsor	Respondents	Key Findings
2009 HIPAA Compliance Review (2009)	CMS	Random sample of 5 CEs for which there were no filed complaints; CMS interviewed senior management as well as individual members of the workforce that received/ processed/ transmitted ePHI	<ul style="list-style-type: none"> <li>• CEs did not perform a risk assessment and did not have a formalized, documented risk assessment process</li> <li>• Risk assessments were outdated and did not address all potential areas of risk</li> <li>• CEs had few and inadequate policies and procedures and they did not address the HIPAA Security Standards and Implementation Specifications</li> <li>• Documented procedures were inconsistent with procedures followed by CE personnel</li> <li>• CEs did not conduct security awareness training prior to granting user access</li> <li>• CEs had BAs but Business Associate Agreements (BAAs) did not exist between the two parties or existing BAAs were inadequate</li> </ul>
2010 HIMSS Analytics Report: Security of Patient Data Commissioned by Kroll Fraud Solutions (December 2009)	HIMSS; Kroll Fraud Solutions	250 executives from health care organizations; included senior information technology (IT) executives, CSOs, and Health Information Management (HIM) Directors/Managers, Compliance Officers, and Privacy Officers	<ul style="list-style-type: none"> <li>• On average, respondents rate their compliance with HITECH/ARRA as 5.75 on a scale of 1-7 (fully compliant)</li> <li>• 66 percent indicated the source of the breach was unauthorized access to information by an individual employed by the organization at the time of the breach</li> <li>• 98 percent have a policy in place to report a breach of patient information</li> <li>• Staff negligence of existing security policies and improper IT security policies were identified as top two causes of data being at risk</li> <li>• Employees were generally unaware of direct costs of data breach</li> <li>• 79 percent responded to a breach by increasing employee training</li> </ul>
2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security (August-September 2009)	HIMSS; ID Experts	150 hospitals and 26 of their BAs; included senior IT executives, CPOs, CSOs, CISOs, and chief medical information officers	<ul style="list-style-type: none"> <li>• Large hospitals are at greatest risk of experiencing data breach, compared to small and medium hospitals</li> <li>• 30 percent of BAs did not know HIPAA Security Requirements had been extended to their organizations</li> <li>• 47 percent of hospitals indicated they would terminate contracts with BAs if patient data was found to be at risk</li> <li>• Compared to providers, BAs lag in all areas of HITECH awareness despite new provisions applying mostly to BAs</li> <li>• Non-IT respondents were more aware of data breaches and HITECH requirements compared to IT respondents, indicating an inter-departmental disconnect at organizations</li> </ul>

© 2011 Deloitte Development LLC. All rights reserved.

**Providers** (hospitals, medical groups, ambulatory facilities, long-term facilities)

Providers' compliance with privacy and security regulations varies based on organization size, technology access, and resource availability.<sup>86</sup> Some large organizations have proactively collaborated with software vendors to develop software that is compliant with HIPAA and other privacy/security regulations.<sup>87</sup> Smaller provider organizations tend to lag, since affordable and interoperable solutions often are unavailable.<sup>88</sup> Cloud-based EMRs could prove a viable solution for small- and medium-sized practices contingent upon resolution of security issues with cloud computing.<sup>89</sup> For all provider organizations, regardless of their size and resources, employee curiosity and subsequent unauthorized access remains a barrier to compliance.<sup>90</sup>

Exacerbating these challenges, several trade associations (AHA, AMA, AAMC, and MGMA) have opined that expanded HIPAA provisions are onerous, disruptive, and overly restrictive.<sup>91,92,93,94</sup> For example, the required accounting of all ePHI disclosures (including those for treatment, billing, and operations) is difficult to collect and maintain, and is rarely requested by patients.<sup>95</sup> Mandating widespread adoption of EHRs poses incremental IT challenges for providers and may impede interoperability. Additionally, current restrictions on the sale of PHI, without patient authorization, profoundly impact and limit research activities. The extra responsibility shifted to providers to manage the downstream privacy and security of PHI could hinder optimal and efficient patient care delivery.<sup>96,97,98,99</sup> For multi-state health care systems, the inconsistency of privacy and security regulations comparing state and federal regulations poses additional risk.<sup>100</sup>

- **Implications for providers:** Regulatory<sup>101,102</sup> and technology changes for data integrity and protection are top priorities for providers.<sup>103</sup> Adequate budget, upper management support, and personnel training are critical to privacy and security initiatives.<sup>104</sup> Preventing unauthorized data access through user sign-on and encryption<sup>105</sup> are risk-minimizing strategies that can be implemented, regardless of practice size. Data protection initiatives also need to extend beyond a provider's own organization to its BAs and their subcontractors.<sup>106,107,108</sup> HHS provides sample BA templates for CEs to ensure proper liability is attributed to BAs and their subcontractors.<sup>109</sup>

**Health Plans** (commercial insurance companies and employer self-insured plans that use an outside agent as its administrative services organization)

The potential for health plan privacy and security data breaches is substantial.<sup>110,111,112</sup> Implementation varies widely within the sector.<sup>113,114</sup> As per HITECH, some health plans' notices of privacy practices are current with ARRA's enhancements to HIPAA, which detail patients' rights to the use and disclosure of their PHI and describe Internet security practices of sharing PHI with external contracted vendors.<sup>115</sup> Many health plans, despite recent data breaches,<sup>116</sup> have outdated notices of privacy practices<sup>117</sup> and lack control over third parties' use of PHI they provide. Forthcoming implementation of HIPAA 5010 (2012) and ICD-10 (2013) assure added risk from expanded security challenges.<sup>118,119,120</sup>

- **Implications for health plans:** Adequate data protection and security are priorities for health plans. Training internal staff, restricting user access, and revising contracts with BAs (and BA subcontractors) to enable secure data handling can reduce data risk.<sup>121,122</sup> Individual accountability and staff awareness of the repercussions of breaches can also help.<sup>123,124</sup>

**Life Sciences** (pharmaceuticals, bio-technology, medical devices, non-allopathic nutraceuticals, functional foods)

Data integrity and security are major risk areas for life sciences organizations (LSOs).<sup>125,126</sup> Copious amounts of routinely collected PHI and financial information are vulnerable to almost daily breaches.<sup>127,128</sup> Internal and external security risks continue to threaten intellectual property critical to LSO competitive advantage.<sup>129</sup> Further, as LSOs look outside the U.S. for emerging markets and cost-containment strategies, data integrity as well as data security issues are becoming more prevalent.<sup>130,131</sup>

HITECH's new limits on CEs' use and sale of PHI impact several operational functions (i.e., market research, clinical trials, patient assistance programs, and pharmacy compliance programs).<sup>132,133</sup> The use of de-identified, secure, and private information by clinical investigators is central to research and development.<sup>134,135</sup> Recently, the International Pharmaceutical Privacy Consortium provided its guidance to HHS, indicating the need to balance individuals' rights to the privacy of their PHI with the societal need for health care research.<sup>136</sup>

• **Implications for life sciences organizations:**

Data protection and security will be an even greater priority for this sector as increasing amounts of sensitive information are collected for LSO operations. Compliance to regulations typically not targeted toward LSOs, such as the Payment Card Industry Data Security Standard (PCI-DSS), will become necessary. Also, protecting intellectual property is paramount. Password protection and email, disc and laptop encryption are important first steps.<sup>137</sup>

**Health information technology solution providers** (hardware, software, application providers, data management, technical support, consulting services, et al.)

The HIT services industry is profoundly impacted as it interacts with all of the players as a "business associate" in the scheme of HIPAA oversight.<sup>138,139</sup> As providers strive to become compliant with privacy and security regulations, they employ a variety of vendors for services and solutions.<sup>140</sup> Technology vendors may support ONC-certified HIT solutions that comply with HHS' technology standards final rule,<sup>141</sup> qualify for CMS' EHR incentives,<sup>142,143,144</sup> and are interoperable with various practice sizes.<sup>145</sup> Service vendors (medical transcriptionists, claims processors, financial services, or any other service with access to PHI),<sup>146</sup> are included in the expanded definition of a BA under HITECH and are liable for data privacy and security in parallel with the CEs they serve.<sup>147</sup> For example, financial institutions providing claims processing and payment services to the health care industry are required to implement technical, physical, and administrative safeguards under HIPAA's security rule in addition to those of the Gramm-Leach-Bliley (GLB) Act<sup>148</sup> they may already have in place.

The push toward a 90 percent EHR adoption rate, implementation of HIPAA 5010, and ICD-10 is likely to increase outsourcing or subcontracting of various data processing activities.<sup>149</sup> Third parties that provide these services may use outdated or less rigorous privacy and security policies and procedures than CEs.<sup>150</sup> Complicating matters, some outsourcing partners operate offshore yet HIPAA is only enforceable in the U.S., so the potential for breaches via PHI handling by non-citizen third parties is an added risk.<sup>151</sup> In fact, few countries have established data privacy and security regulations paralleling the rigor in the U.S., other than the European Union Data Directive and the Swiss Data Protection Act.<sup>152,153</sup>

The HITRUST Alliance, a consortium of health information technology vendors, developed a certifiable security framework (Common Security Framework [CSF]) that can be implemented in any organization regardless of size or security governance maturity.<sup>154</sup> The CSF<sup>155</sup> incorporates current federal, state, third-party, international, and government agency security standards and regulations.<sup>156</sup> The CSF is particularly useful for security self-assessments and to generate risk remediation action plans. Additionally, it is a reputed framework that BAs can implement to demonstrate the quality of their data security practices to CEs.<sup>157</sup>

- **Implications for HIT service providers:** The services industry must ensure greater protection of the PHI it is entrusted with or risk losing substantial amounts of business and relationships.<sup>158</sup> Health care data now crosses multiple industries<sup>159</sup> and borders,<sup>160</sup> and vendors must be aware of the rules for handling PHI. Almost one third of BAs are unaware that new data privacy and security regulations apply to them.<sup>161</sup> Vendors and their subcontractors are now equally liable for data breaches.<sup>162</sup>

“Third-party organizations accounted for 42% of all breaches [in 2010].…”

Source: <http://www.ponemon.org/news-2/23>

### Federal and state government

Federal and state efforts to improve quality and efficiency of care through greater EHR use and the creation of a nationwide health information network (NHIN)<sup>163</sup> are fraught with privacy and security challenges. Health information exchange entails broader access to PHI by numerous entities with varying privacy and security policies.<sup>164</sup> Notably, the Office of the National Coordinator (ONC) for Health Information Technology and the HHS OCR coordinated efforts to ensure that HIE transactions assured optimal privacy and security protections via “meaningful use requirements” for certified EHRs.<sup>165</sup>

Efforts to facilitate federal-state coherency in HIE policies as well as privacy and security are led by the Health Information Security and Privacy Collaboration (HISPC).<sup>166</sup> The resultant “Uniform Security Policy” provides minimum authentication and audit security policies required for operation of statewide HIE.<sup>167</sup>

- **Implications for government:** Federal and state objectives to improve quality and efficiency of health care delivery through EHRs and HIE have tremendous data privacy and security implications. Establishing trust, liability, and standardized data security controls across the exchange will be challenging. Gaining consensus among the multitude of involved entities on minimum necessary privacy and security standards will be critical to establishing trust in this vast exchange of PHI.<sup>168</sup>

### Smart steps for stakeholders

Privacy and security regulations historically have focused on internal security processes; however, in the new normal, culpability has been expanded to downstream entities. As health care delivery transitions to performance-based

compensation, increased transparency, and increased use of EHRs and PHRs, new privacy and security rules, regulations, laws, and standards will be added in each sector. A basic approach to assessing an organization’s current preparedness requires consideration in three key areas (Figure 5):

**Figure 5: Assessing health care organization security and privacy preparedness**

Strategy	Objective	Benefit	Examples
Risk Management <sup>169</sup>	Identify and assess data security risks to develop appropriate security controls to mitigate or avoid risk	Allows health care organizations to make informed decisions on how to allocate security resources to improve data protection	<ul style="list-style-type: none"> <li>Assess current security controls, audit logs, and current policies and procedures</li> <li>Review current BAAs</li> </ul>
Security and Privacy Program	Develop and implement policies, procedures, and training needed to mitigate or avoid risk	Creates baseline standards for the secure handling of sensitive patient information; creates organization-wide awareness of data privacy and security policies	<ul style="list-style-type: none"> <li>Create policies for proper handling of sensitive data; notifying HHS and the media of data breaches</li> <li>Train employees on data handling policies and apply policies to systems that store sensitive data</li> <li>Ensure employees are aware of data handling procedures and notification policies through effective training</li> <li>Modify BAAs to prevent breaches and ensure liability in event of breach</li> <li>Implement safeguards such as data encryption, user- and role-based access and identity management to prevent and limit inappropriate access to PHI</li> <li>Protect information assets and manage data associated risks through an accepted security framework (i.e., HITRUST)</li> </ul>
Compliance	Validate effective risk management and governance	Reduces organizational risk; creates customer trust and confidence in an organization’s protection of PHI; reduces potential for financial penalties due to reasonable cause or willful neglect	<ul style="list-style-type: none"> <li>Demonstrate development and implementation of policies to address identified risks</li> <li>Monitor and log data handling procedures and compliance with established policies</li> <li>Conduct regular internal and third-party security audits and compare reports to internal and external benchmarks that may exist</li> </ul>

© 2011 Deloitte Development LLC. All rights reserved.

A strategic imperative for every organization is a top-management-led, board-approved audit of privacy and security risk, and plans for enhancement.

## Conclusions

Reform will change the U.S. health care system to improve the quality, efficiency, and coordination of health care delivery and payment systems. The “new normal” will be information-driven, connected, and transparent, thus exposing each participant to increased privacy and security risks. This potential liability extends across borders and organizations, with limited operational coherence or technological capabilities. The potential for data breaches is significant and increasing. Stakeholders must act now to prevent compromising sensitive patient data, preserve brand value, and avoid substantial financial penalties for violations.

*All data and information current as of January 2011*

Decreases in internally caused breaches are most likely attributable to internal training programs and employee awareness.

Source: <http://www.ponemon.org/news-2/23>



## References

- 1 Von Bergen, Jane. "Medical data breach said to be major," *Philadelphia Inquirer*, <http://www.philly.com/inquirer/business/105415178.html?page=1&c=y>
- 2 Pritts, JL. "Testimony before the United States House of Representatives Committee on Ways and Means Subcommittee on Health on Health Care Information Technology: Harmonizing Laws Governing the Confidentiality of Health Care Information," July 25, 2005
- 3 "Security and Privacy for Healthcare Providers: Whitepaper, Best Practices Series for Healthcare," Symantec Corporation, 2009
- 4 "Privacy Breach Benchmarks Compel Care Providers to Deploy Breach Monitoring and Commit to a Culture of Privacy and Compliance," a Fairwarning White Paper, Fairwarning Inc., <http://www.fairwarningaudit.com/documents/2010-FAIRWARNING-FINDINGS-REPORT.pdf>. Accessed January 20, 2011
- 5 <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>
- 6 "2010 HIMSS Security Survey," HIMSS, Nov. 3, 2010, [http://www.himss.org/content/files/2010\\_HIMSS\\_SecuritySurvey.pdf](http://www.himss.org/content/files/2010_HIMSS_SecuritySurvey.pdf)
- 7 <http://www.cnn.com/2009/CRIME/10/22/medicare.organized.crime/>
- 8 "2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security," HIMSS, [http://www.himssanalytics.org/docs/ID\\_Experts\\_111509.pdf](http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)
- 9 Pritts, JL. "Testimony before the United States House of Representatives Committee on Ways and Means Subcommittee on Health on Health Care Information Technology: Harmonizing Laws Governing the Confidentiality of Health Care Information," July 25, 2005
- 10 "Comprehensive Privacy and Security: Critical for Health Information Technology," Version 1.0, Center for Democracy and Technology, May 2008, <http://www.cdt.org/healthprivacy/20080514HPframe.pdf>
- 11 Wild KR. "The evolution of HIPAA: the only constant is change," *J Health Care Compliance*, P. 33-36
- 12 McGraw D. Dempsey JX, Harris L, Goldman J. "Privacy as an enabler, not an impediment: building trust into health information exchange," *Health Affairs*, 28(2); 2009: 416-427
- 13 "Issue Brief: Social Networks in Healthcare: Communication, Collaboration and Insights," Deloitte Center for Health Solutions, 2010
- 14 Sharp J. "Social Media in Health Care: Barriers and Future Trends," iHealthbeat, May 2010, <http://www.ihealthbeat.org/perspectives/2010/social-media-in-health-care-barriers-and-future-trends.aspx>. Accessed 11/4/2010
- 15 <http://www.allbusiness.com/health-care/health-care-facilities-hospitals/15356138-1.html>
- 16 Pritts, JL. "Testimony before the United States House of Representatives Committee on Ways and Means Subcommittee on Health on Health Care Information Technology: Harmonizing Laws Governing the Confidentiality of Health Care Information," July 25, 2005
- 17 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act
- 18 "Benchmark Study on Patient Privacy and Data Security," Ponemon Institute, November 9, 2010, <http://www2.idexperts.com/resources/healthcare/healthcare-articles-whitepapers/ponemon-benchmark-study-on-patient-privacy-and-data-security/#>
- 19 "2009 HIPAA Compliance Review Analysis And Summary of Results," Centers for Medicare and Medicaid Services (CMS), Office of E-Health Standards and Services (OEES), September 22, 2009, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev09.pdf>
- 20 "2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security," HIMSS, [http://www.himssanalytics.org/docs/ID\\_Experts\\_111509.pdf](http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)
- 21 "Study shows most health care companies are not ready for new regulations," CroweHorwath, Nov. 11, 2009, <http://www.crowehorwath.com/crowe/news/detail.cfm?id=137>
- 22 Dimitropoulos L, Rizk S. "A state-based approach to privacy and security for interoperable health information exchange," *Health Affairs*, 28 (2) (2009): 428-434
- 23 "Comments on the Department of Health and Human Services' (HHS) proposed rule, 'Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act,'" Medical Group Management Association, September 13, 2010, <http://www.mgma.com/WorkArea/DownloadAsset.aspx?id=39425>
- 24 "2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security," HIMSS, [http://www.himssanalytics.org/docs/ID\\_Experts\\_111509.pdf](http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)
- 25 "2010 HIMSS Analytics Report: Security of Patient Data Commissioned by Kroll Fraud Solutions," HIMSS Analytics, KROLL Fraud Solutions, April 2010, [http://www.krollfraudsolutions.com/media/2010\\_Kroll-HIMSS\\_Study\\_FINAL.pdf](http://www.krollfraudsolutions.com/media/2010_Kroll-HIMSS_Study_FINAL.pdf)
- 26 "Security is not Privacy: Why Current HIT Provisions May Fail," Ingenix white paper, 2010, [http://www.ingenix.com/content/attachments/Ingenix\\_Security-is-Not-Privacy-WhitPaper%20June%202010.pdf](http://www.ingenix.com/content/attachments/Ingenix_Security-is-Not-Privacy-WhitPaper%20June%202010.pdf)
- 27 Ibid
- 28 "The Definition of Business Associate," <http://www.hipaa.com/2009/05/the-definition-of-business-associate/>
- 29 "Covered Entity Charts: Guidance on how to determine whether an organization or individual is a covered entity under the Administrative Simplification provisions of HIPAA," Centers for Medicare and Medicaid Services, <https://www.cms.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf>
- 30 U.S. Department of Health and Human Services, Agency of Healthcare Research and Quality, [http://healthit.ahrq.gov/portal/server.pt/community/privacy\\_and\\_security/1117/what\\_must\\_we\\_do\\_to\\_ensure\\_that\\_our\\_electronic\\_prescriptions\\_are\\_reliably\\_received\\_by\\_the\\_dispensing\\_pharmacy\\_14759](http://healthit.ahrq.gov/portal/server.pt/community/privacy_and_security/1117/what_must_we_do_to_ensure_that_our_electronic_prescriptions_are_reliably_received_by_the_dispensing_pharmacy_14759)
- 31 Dimitropoulos L, Rizk S. "A state-based approach to privacy and security for interoperable health information exchange," *Health Affairs*, 28 (2) (2009): 428-434
- 32 "Security and Privacy for Healthcare Providers: Whitepaper, Best Practices Series for Healthcare," Symantec Corporation, 2009
- 33 "Security is not Privacy: Why Current HIT Provisions May Fail," Ingenix white paper, 2010, [http://www.ingenix.com/content/attachments/Ingenix\\_Security-is-Not-Privacy-WhitPaper%20June%202010.pdf](http://www.ingenix.com/content/attachments/Ingenix_Security-is-Not-Privacy-WhitPaper%20June%202010.pdf)
- 34 McGraw D. Dempsey JX, Harris L, Goldman J. "Privacy as an enabler, not an impediment: building trust into health information exchange," *Health Affairs*, 28(2); 2009: 416-427
- 35 "Issue Brief: Social Networks in Healthcare: Communication, Collaboration and Insights," Deloitte Center for Health Solutions, 2010

- 36 Sharp J. "Social Media in Health Care: Barriers and Future Trends," *iHealthbeat*, May 2010, <http://www.ihealthbeat.org/perspectives/2010/social-media-in-health-care-barriers-and-future-trends.aspx>. Accessed 11/4/2010
- 37 "Information Governance: The Foundation for Effective e-Health," Accenture, [http://www.accenture.com/NR/rdonlyres/E4CE4D61-5C50-475F-9BC8-3185402AA7A8/0/Accenture\\_100473\\_InfoGovPoV\\_Final.pdf](http://www.accenture.com/NR/rdonlyres/E4CE4D61-5C50-475F-9BC8-3185402AA7A8/0/Accenture_100473_InfoGovPoV_Final.pdf)
- 38 McGraw D. Dempsey JX, Harris L, Goldman J. "Privacy as an enabler, not an impediment: building trust into health information exchange," *Health Affairs*, 28(2); 2009: 416-427
- 39 "Issue Brief: Social Networks in Healthcare: Communication, Collaboration and Insights," Deloitte Center for Health Solutions, 2010
- 40 Sharp J. "Social Media in Health Care: Barriers and Future Trends," *iHealthbeat*, May 2010, <http://www.ihealthbeat.org/perspectives/2010/social-media-in-health-care-barriers-and-future-trends.aspx>. Accessed 11/4/2010
- 41 Pritts, JL. "Testimony before the United States House of Representatives Committee on Ways and Means Subcommittee on Health on Health Care Information Technology: Harmonizing Laws Governing the Confidentiality of Health Care Information," July 25, 2005
- 42 "Comprehensive Privacy and Security: Critical for Health Information Technology," Version 1.0, Center for Democracy and Technology, May 2008. <http://www.cdt.org/healthprivacy/20080514HPframe.pdf>
- 43 "OCR Privacy Brief, Summary of the HIPAA Privacy Rule," U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>
- 44 "Summary of the HIPAA Security Rule," U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html>
- 45 "The Health Insurance Portability and Accountability Act (HIPAA) of 1996: Overview and Guidance on Frequently Asked Questions Updated January 24, 2005," Congressional Research Service (CRS) Report for Congress, <http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL3163401242005.pdf>
- 46 Wild KR. "The evolution of HIPAA: the only constant is change," *J Health Care Compliance*, p. 33-36
- 47 Dinh AK. "ARRA's Impact on the Release of PHI," *Managed Care Outlook*, Volume 22, Number 21. Nov. 1, 2009
- 48 "Health Information Privacy," U.S. Department of Health and Human Services. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html>
- 49 "Fact Sheet 8a: HIPAA Basics: Medical Privacy in the Electronic Age," Privacy Rights Clearinghouse, <http://www.privacyrights.org/fs/fs8a-hipaa.htm>
- 50 Bentley L. "HITECH Act means more aggressive HIPAA Enforcement," March 19, 2009, <http://www.itbusinessedge.com/cm/blogs/bentley/hitech-act-means-more-aggressive-hipaa-enforcement/?cs=31212>
- 51 Wild KR. "The evolution of HIPAA: the only constant is change," *J Health Care Compliance*, p. 33-36
- 52 "2010 HIMSS Security Survey," HIMSS, Nov. 3, 2010, [http://www.himss.org/content/files/2010\\_HIMSS\\_SecuritySurvey.pdf](http://www.himss.org/content/files/2010_HIMSS_SecuritySurvey.pdf)
- 53 Toporoff S. "The 'Red Flags' Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft," Federal Trade Commission, <http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm>
- 54 "The Red Flags Rule: What health care businesses need to know," Grant Thornton, [http://www.gt.com/staticfiles/GTCom/Advisory/GRC/Red%20Flags%20materials/Red\\_Flags\\_Rule\\_White\\_Paper\\_Healthcare.pdf](http://www.gt.com/staticfiles/GTCom/Advisory/GRC/Red%20Flags%20materials/Red_Flags_Rule_White_Paper_Healthcare.pdf)
- 55 American Medical Association, Practice Management Center, <http://www.ama-assn.org/ama1/pub/upload/mm/368/red-flags-rule-edu.pdf>
- 56 Toporoff S. "The 'Red Flags' Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft," Federal Trade Commission, <http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm>
- 57 American Medical Association, Practice Management Center, <http://www.ama-assn.org/ama1/pub/upload/mm/368/red-flags-rule-edu.pdf>
- 58 Toporoff S. "The 'Red Flags' Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft," Federal Trade Commission, <http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm>
- 59 American Medical Association, Practice Management Center, <http://www.ama-assn.org/ama1/pub/upload/mm/368/red-flags-rule-edu.pdf>
- 60 <http://www.hipaa.com/>
- 61 "2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security," HIMSS, [http://www.himssanalytics.org/docs/ID\\_Experts\\_111509.pdf](http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)
- 62 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act
- 63 "Health Information Privacy," U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html>
- 64 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act
- 65 "What you need to know about the new HIPAA Breach Notification Rule," American Medical Association, <http://www.ama-assn.org/ama1/pub/upload/mm/399/hipaa-breach-notification-rule.pdf>
- 66 <http://www.ftc.gov/opa/2009/02/cvs.shtm>
- 67 [http://www.healthdatamanagement.com/news/breach\\_hipaa\\_privacy\\_security\\_hitech\\_lawsuit-39645-1.html](http://www.healthdatamanagement.com/news/breach_hipaa_privacy_security_hitech_lawsuit-39645-1.html)
- 68 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act
- 69 "Security is not Privacy: Why Current HIT Provisions May Fail," Ingenix white paper, 2010, [http://www.ingenix.com/content/attachments/Ingenix\\_Security-is-Not-Privacy-WhitPaper%20June%202010.pdf](http://www.ingenix.com/content/attachments/Ingenix_Security-is-Not-Privacy-WhitPaper%20June%202010.pdf)
- 70 "What you need to know about the new HIPAA Breach Notification Rule," American Medical Association, <http://www.ama-assn.org/ama1/pub/upload/mm/399/hipaa-breach-notification-rule.pdf>
- 71 [http://www.hhs.gov/recovery/reports/plans/onc\\_hit.pdf](http://www.hhs.gov/recovery/reports/plans/onc_hit.pdf)

- 72 "HIPAA Survival Guide, HITECH Act Effective Dates," <http://www.hipaasurvivalguide.com/hitech-effective-dates.php>
- 73 U.S. Department of Health and Human Services, Federal Register, Vol. 74, No. 209 / Friday, October 30, 2009 / Rules and Regulations. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf>
- 74 "2010 HIMSS Security Survey," HIMSS, Nov. 3, 2010, [http://www.himss.org/content/files/2010\\_HIMSS\\_SecuritySurvey.pdf](http://www.himss.org/content/files/2010_HIMSS_SecuritySurvey.pdf)
- 75 "2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security," HIMSS, [http://www.himssanalytics.org/docs/ID\\_Experts\\_111509.pdf](http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)
- 76 "Benchmark Study on Patient Privacy and Data Security," Ponemon Institute, November 9, 2010, <http://www2.idexperts.com/resources/healthcare/healthcare-articles-whitepapers/ponemon-benchmark-study-on-patient-privacy-and-data-security/#>
- 77 "2009 HIPAA Compliance Review Analysis and Summary of Results," Centers for Medicare and Medicaid Services (CMS), Office of E-Health Standards and Services (OEES), September 22, 2009, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev09.pdf>
- 78 "2010 HIMSS Analytics Report: Security of Patient Data Commissioned by Kroll Fraud Solutions," HIMSS Analytics, KROLL Fraud Solutions, April 2010, [http://www.krollfraudsolutions.com/media/2010\\_Kroll-HIMSS\\_Study\\_FINAL.pdf](http://www.krollfraudsolutions.com/media/2010_Kroll-HIMSS_Study_FINAL.pdf)
- 79 "Slow Hospital Compliance with New Regulations Causing Increased Data Breaches & Medical Identity Theft," Spring 2010 National Survey of Hospital Compliance Executives, [http://www.identityforce.com/tools/press/Identity\\_Force\\_Spring\\_2010\\_Hospital\\_Compliance\\_Report\\_April\\_20\\_2010.pdf](http://www.identityforce.com/tools/press/Identity_Force_Spring_2010_Hospital_Compliance_Report_April_20_2010.pdf)
- 80 "2010 HIMSS Security Survey," HIMSS, Nov. 3, 2010, [http://www.himss.org/content/files/2010\\_HIMSS\\_SecuritySurvey.pdf](http://www.himss.org/content/files/2010_HIMSS_SecuritySurvey.pdf)
- 81 "2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security," HIMSS, [http://www.himssanalytics.org/docs/ID\\_Experts\\_111509.pdf](http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)
- 82 "Benchmark Study on Patient Privacy and Data Security," Ponemon Institute, November 9, 2010, <http://www2.idexperts.com/resources/healthcare/healthcare-articles-whitepapers/ponemon-benchmark-study-on-patient-privacy-and-data-security/#>
- 83 "2009 HIPAA Compliance Review Analysis and Summary of Results," Centers for Medicare and Medicaid Services (CMS), Office of E-Health Standards and Services (OEES), September 22, 2009, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev09.pdf>
- 84 "2010 HIMSS Analytics Report: Security of Patient Data Commissioned by Kroll Fraud Solutions," HIMSS Analytics, KROLL Fraud Solutions, April 2010. [http://www.krollfraudsolutions.com/media/2010\\_Kroll-HIMSS\\_Study\\_FINAL.pdf](http://www.krollfraudsolutions.com/media/2010_Kroll-HIMSS_Study_FINAL.pdf)
- 85 "Slow Hospital Compliance with New Regulations Causing Increased Data Breaches & Medical Identity Theft," Spring 2010 National Survey of Hospital Compliance Executives, [http://www.identityforce.com/tools/press/Identity\\_Force\\_Spring\\_2010\\_Hospital\\_Compliance\\_Report\\_April\\_20\\_2010.pdf](http://www.identityforce.com/tools/press/Identity_Force_Spring_2010_Hospital_Compliance_Report_April_20_2010.pdf)
- 86 "Comments on the Department of Health and Human Services' (HHS) proposed rule, 'Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act,'" Medical Group Management Association, September 13, 2010, <http://www.mgma.com/WorkArea/DownloadAsset.aspx?id=39425>
- 87 "Comments on the Department of Health and Human Service's guidance specifying the technologies and methodologies that render protected health information (PHI) unusable, unreadable, or indecipherable to unauthorized individuals to prevent triggering the breach notification requirements specified in the recently enacted 'American Recovery and Reinvestment Act of 2009' (ARRA) (Pub. L. 111-5)," American Medical Association, <http://www.ama-assn.org/ama1/pub/upload/mm/368/phi-letter.pdf>
- 88 "Re: RIN 0991-AB57; Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed. Reg. 40868 (July 14, 2010)," American Hospital Association, September 10, 2010, <http://www.aha.org/aha/letter/2010/100910-cl-HIPAA-HITECH.pdf>
- 89 <http://www.hipaa.com/>
- 90 <http://www.healthleadersmedia.com/content/HR-230986/Octomom-Records-Breach-a-Lesson-in-Patient-Privacy>
- 91 "Comments on the Department of Health and Human Services' (HHS) proposed rule, 'Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act,'" Medical Group Management Association, September 13, 2010, <http://www.mgma.com/WorkArea/DownloadAsset.aspx?id=39425>
- 92 "Comments on the Department of Health and Human Service's guidance specifying the technologies and methodologies that render protected health information (PHI) unusable, unreadable, or indecipherable to unauthorized individuals to prevent triggering the breach notification requirements specified in the recently enacted 'American Recovery and Reinvestment Act of 2009' (ARRA) (Pub. L. 111-5)," American Medical Association, <http://www.ama-assn.org/ama1/pub/upload/mm/368/phi-letter.pdf>
- 93 "Re: RIN 0991-AB57; Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed. Reg. 40868 (July 14, 2010)," American Hospital Association, September 10, 2010, <http://www.aha.org/aha/letter/2010/100910-cl-HIPAA-HITECH.pdf>
- 94 "Comments in response to the Request for Information (RFI), *HIPAA Privacy Rule Accounting for Disclosures Under the Health Information Technology for Economic and Clinical Health Act*, 75 Fed. Reg. 23214," Association of American Medical Colleges of America, May 18, 2010, [https://www.aamc.org/download/121152/data/aamc\\_commentletter\\_ocr-hitechdisclosures.pdf.pdf](https://www.aamc.org/download/121152/data/aamc_commentletter_ocr-hitechdisclosures.pdf.pdf)
- 95 Cadet J. "MGMA: New HIPAA disclosure requirements are too costly, burdensome," May 19, 2010, [http://www.cmio.net/index.php?option=com\\_articles&article=22251&publication=68&view=portals](http://www.cmio.net/index.php?option=com_articles&article=22251&publication=68&view=portals)
- 96 "Comments on the Department of Health and Human Services' (HHS) proposed rule, 'Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act,'" Medical Group Management Association, September 13, 2010, <http://www.mgma.com/WorkArea/DownloadAsset.aspx?id=39425>
- 97 "Comments on the Department of Health and Human Service's guidance specifying the technologies and methodologies that render protected health information (PHI) unusable, unreadable, or indecipherable to unauthorized individuals to prevent triggering the breach notification requirements specified in the recently enacted 'American Recovery and Reinvestment Act of 2009' (ARRA) (Pub. L. 111-5), American Medical Association, <http://www.ama-assn.org/ama1/pub/upload/mm/368/phi-letter.pdf>
- 98 "Re: RIN 0991-AB57; Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed. Reg. 40868 (July 14, 2010)," American Hospital Association, September 10, 2010. <http://www.aha.org/aha/letter/2010/100910-cl-HIPAA-HITECH.pdf>
- 99 Cadet J. "MGMA: New HIPAA disclosure requirements are too costly, burdensome," May 19, 2010, [http://www.cmio.net/index.php?option=com\\_articles&article=22251&publication=68&view=portals](http://www.cmio.net/index.php?option=com_articles&article=22251&publication=68&view=portals)

- 100 "Comments on the Department of Health and Human Services' (HHS) proposed rule, 'Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act,'" Medical Group Management Association, September 13, 2010, <http://www.mgma.com/WorkArea/DownloadAsset.aspx?id=39425>
- 101 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act
- 102 The Patient Protection and Affordable Care Act of 2010 (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010
- 103 Degaspari J. "Staying ahead of the curve on data security," *HealthCare Informatics*, October 2010, <http://www.healthcareinformatics.com/ME2/dirmod.aspx?sid=&nm=&type=Publishing&mod=mod=Publications%3A%3AArticle&mid=8F3A7027421841978f188E895F87F791&tier=4&id=35F1496AE0B144D3A9716D5D9C2D03CF>
- 104 "Benchmark Study on Patient Privacy and Data Security," Ponemon Institute, November 9, 2010, <http://www2.idexperts.com/resources/healthcare/healthcare-articles-whitepapers/ponemon-benchmark-study-on-patient-privacy-and-data-security/#>
- 105 <http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/technologymethods.html>
- 106 "2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security," HIMSS, [http://www.himssanalytics.org/docs/ID\\_Experts\\_111509.pdf](http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)
- 107 "2009 HIPAA Compliance Review Analysis and Summary of Results," Centers for Medicare and Medicaid Services (CMS), Office of E-Health Standards and Services (OESS), September 22, 2009, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliance09.pdf>
- 108 Degaspari J. "Staying ahead of the curve on data security," *HealthCare Informatics*, October 2010, <http://www.healthcareinformatics.com/ME2/dirmod.aspx?sid=&nm=&type=Publishing&mod=mod=Publications%3A%3AArticle&mid=8F3A7027421841978f188E895F87F791&tier=4&id=35F1496AE0B144D3A9716D5D9C2D03CF>
- 109 <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>
- 110 <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>
- 111 <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>
- 112 <http://www.healthleadersmedia.com/page-1/TEC-259666/OCR-Data-Breaches-Double-Since-July##>
- 113 [http://www.uhc.com/privacy/notice\\_of\\_privacy\\_practices.htm](http://www.uhc.com/privacy/notice_of_privacy_practices.htm). Accessed 11/4/10
- 114 [http://www.wellpoint.com/privacy\\_policy.asp](http://www.wellpoint.com/privacy_policy.asp). Accessed 11/4/10
- 115 [http://www.uhc.com/privacy/notice\\_of\\_privacy\\_practices.htm](http://www.uhc.com/privacy/notice_of_privacy_practices.htm). Accessed 11/4/10
- 116 <http://www.ihealthbeat.org/articles/2010/11/2/indiana-attorney-general-sues-health-insurer-over-data-breach.aspx>. Accessed 11/4/10
- 117 [http://www.wellpoint.com/privacy\\_policy.asp](http://www.wellpoint.com/privacy_policy.asp). Accessed 11/4/10
- 118 [http://www.ingenixconsulting.com/HealthCareInsights/Insight/CD10HIPAA5010/insight\\_122/](http://www.ingenixconsulting.com/HealthCareInsights/Insight/CD10HIPAA5010/insight_122/)
- 119 [http://www.ingenixconsulting.com/content/File/Leveraging\\_ICD-10\\_for\\_Strategic\\_Advantage.pdf](http://www.ingenixconsulting.com/content/File/Leveraging_ICD-10_for_Strategic_Advantage.pdf)
- 120 [http://www.emdeon.com/5010/pdfs/HIPAA\\_Simplified\\_FAQ\\_I-5010.pdf](http://www.emdeon.com/5010/pdfs/HIPAA_Simplified_FAQ_I-5010.pdf)
- 121 "2009 HIPAA Compliance Review Analysis and Summary of Results," Centers for Medicare and Medicaid Services (CMS), Office of E-Health Standards and Services (OESS), September 22, 2009, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliance09.pdf>
- 122 "2010 HIMSS Analytics Report: Security of Patient Data Commissioned by Kroll Fraud Solutions," HIMSS Analytics, KROLL Fraud Solutions, April 2010. [http://www.krollfraudsolutions.com/media/2010\\_Kroll-HIMSS\\_Study\\_FINAL.pdf](http://www.krollfraudsolutions.com/media/2010_Kroll-HIMSS_Study_FINAL.pdf)
- 123 "2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security," HIMSS, [http://www.himssanalytics.org/docs/ID\\_Experts\\_111509.pdf](http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)
- 124 "2010 HIMSS Analytics Report: Security of Patient Data Commissioned by Kroll Fraud Solutions," HIMSS Analytics, KROLL Fraud Solutions, April 2010. [http://www.krollfraudsolutions.com/media/2010\\_Kroll-HIMSS\\_Study\\_FINAL.pdf](http://www.krollfraudsolutions.com/media/2010_Kroll-HIMSS_Study_FINAL.pdf)
- 125 [http://www.pharmatimes.com/Article/10-01-18/Charges\\_levelled\\_in\\_Reuben\\_data\\_fraud\\_case.aspx](http://www.pharmatimes.com/Article/10-01-18/Charges_levelled_in_Reuben_data_fraud_case.aspx)
- 126 <http://www.whistleblowerfirm.com/about/published-articles/pharmcomp/>
- 127 [http://www.cio.com/article/492240/The\\_Inside\\_Story\\_of\\_a\\_Shocking\\_Data\\_Leak\\_Audit\\_?page=1&taxonomyId=3089](http://www.cio.com/article/492240/The_Inside_Story_of_a_Shocking_Data_Leak_Audit_?page=1&taxonomyId=3089)
- 128 <http://www.information-age.com/channels/information-management/news/1303198/were-drowning-in-data-says-pharma-giant-roche.shtml>
- 129 <http://www.kpmg.com/Global/en/WhatWeDo/Industries/Pharmaceuticals/Pages/The-pharmaceutical-industry-fraud.aspx>
- 130 <http://www.pharmamanufacturing.com/industrynews/2008/144.html>
- 131 <http://www.pharma-mag.com/News/tabid/63/EntryId/125/Cost-Benefits-and-Considerable-Scientific-Expertise-Provide-China-Strategic-Advantage-for-Drug-Discovery-Outsourcing.aspx>
- 132 Peddicord D, Waldo AB, Boutin M, Grande T, Gutierrez L. "A proposal to protect privacy of health information while accelerating comparative effectiveness research," *Health Affairs*, 29, No. 11(2010): 2082-2090
- 133 <http://www.mondaq.com/unitedstates/article.asp?articleid=105784>
- 134 Peddicord D, Waldo AB, Boutin M, Grande T, Gutierrez L. "A proposal to protect privacy of health information while accelerating comparative effectiveness research," *Health Affairs*, 29, No. 11(2010): 2082-2090
- 135 <http://www.ecliniqua.com/2010/1/4/hipaa2.html>
- 136 <http://www.pharmaprivacy.org/download/IPPC%20Comments%20to%20HHS%20re%20RIN%200991-AB57.pdf>
- 137 [http://www.cio.com/article/492240/The\\_Inside\\_Story\\_of\\_a\\_Shocking\\_Data\\_Leak\\_Audit\\_?page=2&taxonomyId=3089](http://www.cio.com/article/492240/The_Inside_Story_of_a_Shocking_Data_Leak_Audit_?page=2&taxonomyId=3089)

- 138 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act
- 139 Degaspari J. "Staying ahead of the curve on data security," *HealthCare Informatics*, October 2010, <http://www.healthcareinformatics.com/ME2/dirmod.asp?sid=&nm=&type=Publishing&mod=mod=Publications%3A%3AArticle&mid=8F3A7027421841978f18BE895F87F791&tier=4&id=35F1496AE0B144D3A9716D5D9C2D03CF>
- 140 <http://www.outsourcing-center.com/2010-01-upcoming-challenges-and-opportunities-in-healthcare-outsourcing-article-37464.html>
- 141 According to HHS' Technology Standards Final Rule, EHR software must contain security functions such as data encryption, auditing capabilities, including read-only access to patient records, automatic log-off, and file and message integrity checking.
- 142 <http://sites.mckesson.com/AchieveHIT/ehrsolutions.asp>
- 143 <http://investor.allscripts.com/phoenix.zhtml?c=112727&p=RssLanding&cat=news&id=1479007>
- 144 <http://www.thestreet.com/story/10911507/1/ge-centricity174-enterprise-achieves-20112012-certification.html>
- 145 "Comments on the Department of Health and Human Services' (HHS) proposed rule, 'Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act,'" Medical Group Management Association, September 13, 2010, <http://www.mgma.com/WorkArea/DownloadAsset.aspx?id=39425>
- 146 "Personal Health Information: Privacy and Security Considerations in Outsourcing and Offshoring Decisions," TPI, June 2007, <http://www.tpi.net/pdf/papers/Personal%20Health%20Information.pdf>
- 147 <http://www.mondaq.com/unitedstates/article.asp?articleid=105784>
- 148 Malek LA, Naser C, Servello SJ, Stone S. "Why Should Banks Care About Healthcare Reform?" *ABA Bank Compliance*, Jul/Aug 2010, p. 32
- 149 <http://www.outsourcing-center.com/2010-01-upcoming-challenges-and-opportunities-in-healthcare-outsourcing-article-37464.html>
- 150 <http://www.virsci.com/privacyconsult.html>
- 151 <http://www.healthdatamanagement.com/issues/20050201/10505-1.html>
- 152 [http://markey.house.gov/docs/privacy/iss\\_privacy\\_rep050914.pdf](http://markey.house.gov/docs/privacy/iss_privacy_rep050914.pdf)
- 153 <http://bjl.ucdavis.edu/archives/vol-6-no-2/Offshore-Outsourcing-to-India.html>
- 154 "The HITRUST Common Security Framework: A revolutionary way to protect electronic health information," HITRUST, <http://www.hitrustalliance.net/HITRUST%20CSF%20Brochure.pdf>
- 155 Security standards incorporated into HITRUST's CSF include: Federal- HIPAA, HITECH; Third party- Payment Card Industry (PCI) and the Control Objectives for Information and related Technology (COBIT); International- International Standards Organization (ISO); Governmental Agencies- Centers for Medicare and Medicaid Services (CMS), Federal Trade Commission (FTC), and National Institute of Standards and Technology (NIST).
- 156 <http://www.hitrustalliance.net/>
- 157 <http://www.hitrustalliance.net/HITRUST%20CSF%20Assurance%20Program.pdf>
- 158 2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security, HIMSS, [http://www.himssanalytics.org/docs/ID\\_Experts\\_111509.pdf](http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)
- 159 Degaspari J. "Staying ahead of the curve on data security," *HealthCare Informatics*, October 2010, <http://www.healthcareinformatics.com/ME2/dirmod.asp?sid=&nm=&type=Publishing&mod=mod=Publications%3A%3AArticle&mid=8F3A7027421841978f18BE895F87F791&tier=4&id=35F1496AE0B144D3A9716D5D9C2D03CF>
- 160 <http://www.healthdatamanagement.com/issues/20050201/10505-1.html>
- 161 "2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security," HIMSS, [http://www.himssanalytics.org/docs/ID\\_Experts\\_111509.pdf](http://www.himssanalytics.org/docs/ID_Experts_111509.pdf)
- 162 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act
- 163 [http://healthit.hhs.gov/portal/server.pt?CommunityID=2994&spaced=11&parentname=CommunityEditor&control=SetCommunity&parentid=9&in\\_hi\\_userid=11673&PageID=0&space=CommunityPagev](http://healthit.hhs.gov/portal/server.pt?CommunityID=2994&spaced=11&parentname=CommunityEditor&control=SetCommunity&parentid=9&in_hi_userid=11673&PageID=0&space=CommunityPagev)
- 164 Dimitropoulos L, Rizk S. "A state-based approach to privacy and security for interoperable health information exchange," *Health Affairs*, 28 (2) (2009): 428-434
- 165 [http://healthit.hhs.gov/portal/server.pt?CommunityID=2994&spaced=11&parentname=CommunityEditor&control=SetCommunity&parentid=9&in\\_hi\\_userid=11673&PageID=0&space=CommunityPagev](http://healthit.hhs.gov/portal/server.pt?CommunityID=2994&spaced=11&parentname=CommunityEditor&control=SetCommunity&parentid=9&in_hi_userid=11673&PageID=0&space=CommunityPagev)
- 166 Dimitropoulos L, Rizk S. "A state-based approach to privacy and security for interoperable health information exchange," *Health Affairs*, 28 (2) (2009): 428-434
- 167 "Guide to Adoption of Uniform Security Policy," Health Information Security and Privacy Collaboration, March 31, 2009
- 168 Dimitropoulos L, Rizk S. "A state-based approach to privacy and security for interoperable health information exchange," *Health Affairs*, 28 (2) (2009): 428-434
- 169 Risk assessment is a mandatory requirement of the HIPAA Security Rule as well as part of the Stage 1 Meaningful Use criteria.

## Authors

Paul H. Keckley, PhD  
Executive Director  
Deloitte Center for Health Solutions  
Deloitte LLP  
pkeckley@deloitte.com

Sheryl Coughlin, PhD, MHA  
Research Leader  
Deloitte Center for Health Solutions  
Deloitte LLP  
scoughlin@deloitte.com

Shiraz Gupta, PharmD, MPH  
Senior Research Manager  
Deloitte Center for Health Solutions  
Deloitte LLP  
shirazgupta@deloitte.com

## Contributors

Mark Ford  
Principal  
Deloitte & Touche LLP  
mford@deloitte.com

Deborah Golden  
Principal  
Deloitte & Touche LLP  
debgolden@deloitte.com

Bruce Murphy  
Principal  
Deloitte & Touche LLP  
brmurphy@deloitte.com

Todd Shock  
Specialist Leader  
Deloitte Consulting LLP  
tshock@deloitte.com

David Steier  
Director  
Deloitte Consulting LLP  
dsteier@deloitte.com

Kenneth Weixel  
Partner  
Deloitte & Touche LLP  
kweixel@deloitte.com

## Acknowledgements

We wish to thank Derek Han, Seda Cinlar, Mark Schutzmann, and Priyum Jyoti for their contributions to this paper as well as Jennifer Bohn, Kerry Iseman, and the many others who contributed their ideas and insights during the design, analysis, and reporting stages of this project.

## Contact information

To learn more about the Deloitte Center for Health Solutions, its projects and events, please visit:  
[www.deloitte.com/centerforhealthsolutions](http://www.deloitte.com/centerforhealthsolutions).

Deloitte Center for Health Solutions  
555 12th Street N.W.  
Washington, DC 20004  
Phone 202-220-2177  
Fax 202-220-2178  
Toll free 888-233-6169  
Email [healthsolutions@deloitte.com](mailto:healthsolutions@deloitte.com)  
Web <http://www.deloitte.com/centerforhealthsolutions>

# Deloitte.

## Center for Health Solutions

### **About the Center**

The Deloitte Center for Health Solutions (DCHS) is the health services research arm of Deloitte LLP. Our goal is to inform all stakeholders in the health care system about emerging trends, challenges and opportunities using rigorous research. Through our research, roundtables and other forms of engagement, we seek to be a trusted source for relevant, timely and reliable insights.

To learn more about the DCHS, its research projects and events, please visit:  
[www.deloitte.com/centerforhealthsolutions](http://www.deloitte.com/centerforhealthsolutions)

Copyright © 2011 Deloitte Development LLC. All rights reserved.

Member of Deloitte Touche Tohmatsu Limited

These materials and the information contained herein are provided by Deloitte LLP and are intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subject(s). Accordingly, the information in these materials is not intended to constitute accounting, tax, legal, investment, consulting or other professional advice or services. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional advisor.

These materials and the information contained therein are provided as is, and Deloitte LLP makes no express or implied representations or warranties regarding these materials or the information contained therein. Without limiting the foregoing, Deloitte LLP does not warrant that the materials or information contained therein will be error-free or will meet any particular criteria of performance or quality. Deloitte LLP expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, non-infringement, compatibility, security and accuracy.

Your use of these materials and information contained therein is at your own risk, and you assume full responsibility and risk of loss resulting from the use thereof. Deloitte LLP will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials or the information contained therein.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.

### **About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2011 Deloitte Development LLC. All rights reserved.

Member of Deloitte Touche Tohmatsu Limited