

**Deloitte.**

**ORACLE®**

*Securing Electronic Health Records (EHRs)  
to Achieve “Meaningful Use” Compliance,  
Prevent Data Theft and Fraud*

Featuring the results of the

**Healthcare IT News**

**Privacy and Security Survey, March 2011**

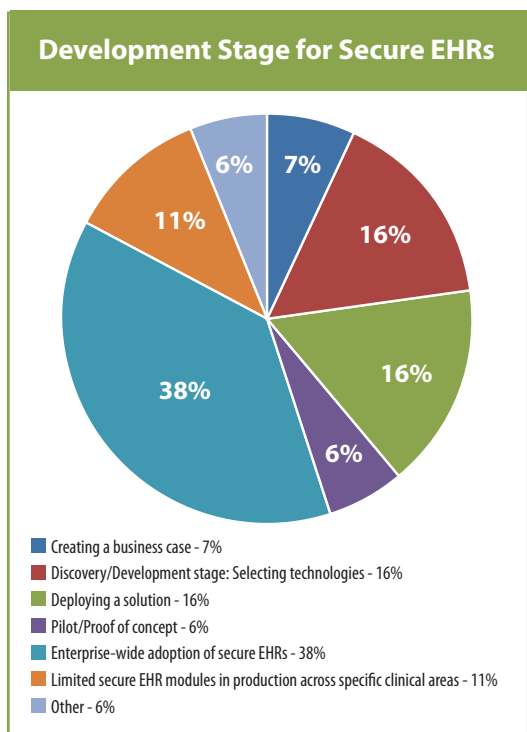


Since the passage of the HITECH Act, under the American Recovery and Reinvestment Act of 2009, efforts toward EHR adoption have increased significantly. Eighty-one percent of hospitals expressed their intent to qualify for payments under the Medicare and Medicaid EHR Incentive Programs, with about two-thirds expecting to enroll during the first stage of Meaningful Use (MU) in 2011-2012, according to the 2010 American Hospital Association’s Annual Survey Database.

A considerable amount of healthcare providers’ time and resources have been devoted to getting the basic EHR foundation in place. Meeting the objectives and measures for improving quality, safety, efficiency, care coordination, population and public health are getting the most attention within the core set of the Stage 1 MU criteria. While providing adequate privacy and security protections for personal health information is also a core set goal, healthcare providers seem to be only now realizing the need to establish a secure EHR system.

As a result of the primary focus on getting EHRs operational, in many cases healthcare providers may have overlooked or ignored putting in place security and privacy protections. This was one of the key findings in a March 2011 *Healthcare IT News* survey, which was conducted on behalf of Oracle Corporation (Oracle) and Deloitte<sup>1</sup> to determine the knowledge and activity of hospitals and health systems around securing EHRs for achieving both MU compliance and preventing data theft and fraud. Nearly 300 individuals participated, with nearly a third holding the position of IT director or manager. The rest comprised CIOs or CTOs, administrative directors or managers, CMIOs, and privacy and security managers, among others.

“For the most part, healthcare providers have relied on vendors that support EHR technology to have the appropriate confidentiality, integrity and availability controls in place,” said Danny Rojas, senior manager, Security & Privacy services, at Deloitte. In addition, security traditionally has been thought of as an enterprise-level service, separate from the EHR implementation, added Reid Oakes, senior director, Healthcare and Life Sciences Technology Solutions, at Oracle. The HITECH Act and the Patient Protection and Affordability Care Act (PPACA) of 2010 have added more rigor and regulatory pressure to establishing a trust framework for patient data that resides in the EHR, Rojas said. “We’re now seeing a convergence around the need for security as part of the EHR process,” Oakes said.



The EHR Incentive Program Final Rule requires healthcare providers to establish privacy and security protections for confidential information through operating policies, procedures, and technologies and compliance with applicable law, and deliver data-sharing transparency to patients. In addition, it calls for protecting electronic health information created or maintained by the certified EHR technology systems through the deployment of appropriate technical capabilities, which correspond to certification criteria for EHR technology. Secure EHRs comply with the Final Rule, but they also employ robust controls such as multi-level authentication and authorization, identity proofing, patient data access management and fraud detection to help healthcare providers significantly improve their privacy and security practices overall<sup>1</sup>.

### Striving for Compliance, Yet Critical Mass Lacking on Security

For 80 percent of the *Healthcare IT News* survey respondents, meeting compliance was the highest expectation of achieving meaningful use of EHRs, followed by improved quality of care (71 percent), patient safety (67 percent) and cost savings (43 percent). Only 38 percent of respondents, however, reported that they are currently in the process of enterprise-wide adoption of secure EHRs. While this “advanced” activity is promising, the percentage of

<sup>1</sup> As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary 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. Certain services may not be available to attest clients under the rules and regulations of public accounting.

respondents engaged in implementing a higher level of secure EHRs is low, especially given that qualification for Stage 1 incentive payments began this year.

The remaining respondents reported that their organizations are in earlier stages of developing secure EHRs. Only 16 percent of respondents indicated that their organizations are deploying a solution for the development of a secure EHR. Another 16 percent are in the discovery/development stage and as such are in the midst of selecting technologies. Eleven percent have limited secure EHR modules in production across specific clinical areas. Seven percent are in the process of creating a business case, while 6 percent specified other, which included not having a plan at all. Awareness may be prevalent, but these data points suggest that healthcare providers need to act more swiftly. Securing EHRs meets multiple MU criteria, a fact that should spur action on the part of those who are far behind.

### **Driving Adoption, Increasing Efficiency and Decreasing Costs**

Before clinicians can meaningfully use EHRs, they must overcome the traditional adoption barriers, including cost, lack of usability, productivity loss and workflow disruption. A cumbersome and manually driven privacy and security infrastructure can exacerbate those barriers. According to 59 percent of survey respondents, their healthcare organizations use their helpdesks to manually manage updating access when employees' job roles change. Reliance on manual processes, which negatively impacts user experience and drives up IT costs, confirms what Oracle is seeing in the market, Oakes said.

"The key to the strategy is security should not get in the way of the clinical process," he said. "Healthcare providers must not overcomplicate the clinicians' environment and instead find easy ways to build, for example, comprehensive models for role assignments. Solving and automating identity creation and management processes, and solidifying those workflows upfront will deliver a seamless EHR experience for clinicians, which will make adoption more feasible and increase patient satisfaction as clinicians spend more time on patients rather than logging on or trying to access applications on their electronic devices," Oakes said.

***Nonetheless, expect the number of healthcare organization participation in HIEs to increase significantly when the exchange of clinical data among separate entities takes on a greater role in stages 2 and 3 MU criteria."***

**REID OAKES**

*Senior Director, Healthcare and Life Sciences Technology Solutions*

**Oracle**

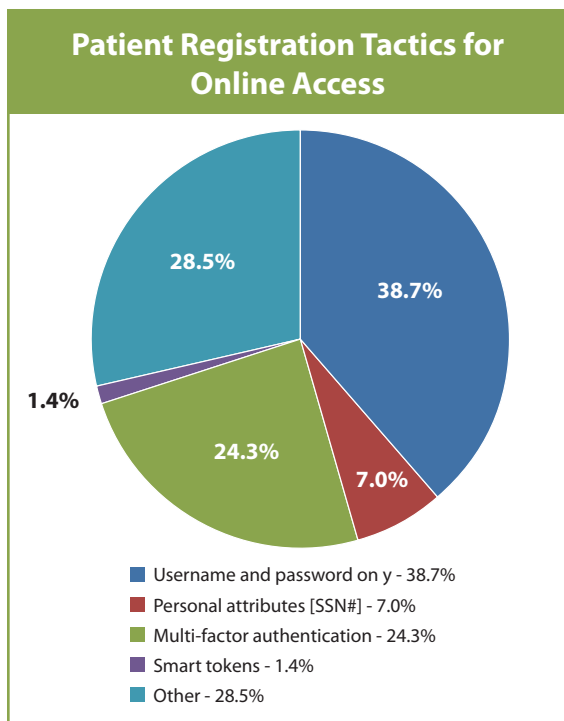
Automating identity management processes will also save costs during implementation by avoiding increased resources required for manual creation of identities and certification of privileges and roles. "If you don't take care of all the identity management and access controls, you can incur costs and increase volume to helpdesks," said Oakes. Lack of controls can give rise to password and single-sign on issues, such as poor password choices. "Unless you lock down that part and automate it, you're really just going to shift the cost," he said.

### **Controlling Risks Outside the Enterprise**

MU criteria require healthcare providers to offer their patients an electronic copy of their health information and be able to exchange key clinical information to improve care coordination. Both criteria involve sending patient data outside of a healthcare provider's

# **H** *Healthcare providers need to think at an enterprise level about what staff members are doing with the data and create a fraud-detection construct around how people get access to data."*

enterprise, which demands another level of rigorous privacy and security controls. Less than half of respondents reported that their organizations provide online access to patient records today. While 24 percent use multi-factor authentication to verify user identity or legitimacy of the transaction, 39 percent deploy username and password only to securely register patients for online access. More healthcare providers are granting online access to patient records, to be in compliance with MU. While more robust access controls, such as multi-factor authentication and adaptive access control to monitor user behavior, are not required overall, they are highly recommended especially if healthcare providers believe they are at a higher risk for privacy breaches and data theft.



More than a third of survey respondents share patient data with other organizations over a secure electronic network, and 23 percent use a health information exchange's (HIE) secure electronic network. Many HIEs and regional health information organizations (RHIOs) are still struggling with establishing sustainable business models and achieving critical mass of data-sharing partners whose contributions would create a broader, deeper and richer set of data. These usage numbers are encouraging, signaling HIE's value proposition to healthcare providers. The privacy and security risks and complexities increase, however, as the number of data-sharing partners grows within and outside of HIEs and RHIOs.

"Nonetheless, expect the number of healthcare organization participation in HIEs to increase significantly when the exchange of clinical data among separate entities takes on a greater role in stages 2 and 3 MU criteria," Oakes said. "As healthcare providers engage in HIE activity, they will need to deploy information rights management, which helps to ensure that once the data leaves the organization it is properly secured with the appropriate levels of security embedded to prevent data breaches and theft, as in the case of stolen electronic devices." In general security has to become more context aware and more granular to secure private data while allowing clinicians access to data that they need to be productive.

## **Eliminating Privacy Breaches and Data Theft, Detecting Fraud Within the Enterprise**

Healthcare providers must also implement policies and controls to protect patient data within their four walls. The national media have reported on numerous privacy breaches in which hospital staff inappropriately accessed celebrities' EHRs. A well-known Southern California medical center incurred multiple breaches involving the same pop singer in 2005 and 2008. More recently, three clinical support staff members at the Tucson University Medical Center were fired in January 2011 after allegedly accessing patient records of victims of the shooting tragedy in Arizona, which included U.S. Representative Gabrielle Giffords (D-AZ).

Enabling the right people to see the right data at the right time within the healthcare organization requires robust access control policies and applications. According to the survey, nearly three-fourths of the respondents employ role-based control methods to

manage patient data access, followed by 13 percent whose organizations use mandatory access control. More than a third employ multi-factor authentication to perform identity proofing, followed by 27 percent whose organizations provide in-house background checking and 26 percent who deploy knowledge-based authentication. Implementing the right level of security provisioning, entitlement and other controls will ensure healthcare providers are protecting data within their organization. "Access management has a major play in how we respond to meaningful use requirements," Oakes said. A security inside-out approach, which Oracle deploys, can help to secure and manage the data where it resides, as well as when it gets pushed out to and beyond the application level.

Role-based security controls, internal policies and audit trails can help address privacy breach risks. Healthcare providers should also consider employing preventive and detective approaches to review user access, determine risk, and prevent excessive access to private data. Should a privacy breach occur, healthcare providers can rely on audit trails to identify who improperly accessed patient data and take immediate action dictated by internal policies. Proper policies and technical capabilities that enable a swift response can mitigate damage to and even enhance the healthcare provider's standing, which is critical in today's competitive market.

While 62 percent of respondents use security information and event management (SIEM) and 13 percent deploy data leakage prevention tools to protect online patient data, a quarter of respondents have no fraud detection solution in place, which can increase vulnerability to fraud and the risk of noncompliance. "Healthcare providers need to think at an enterprise level about what staff members are doing with the data and create a fraud-detection construct around how people get access to data," Oakes said. For example, clinicians as a group would be expected to have access to patient records. However, only clinicians assigned to a patient's care team should have access to that particular patient's record. Historically, identity and security have been managed at the enterprise level. With the adoption of EHRs, healthcare providers need to integrate privacy and security at the clinical application level, but still leverage some enterprise-class services.

**H**ITRUST is really looking to provide common set of prescriptive security requirements that allow multiple healthcare players achieve a common goal relative to their own security posture and to meet HIPAA security rule compliance."

**MARK FORD**

*Principal, Security & Privacy Services, Healthcare Services*  
**Deloitte & Touche LLP**

### **Meeting HIPAA and Certification Requirements**

The HITECH Act increased Health Insurance Portability and Accountability Act's (HIPAA) data privacy and security requirements and expanded responsibility to business associates of covered entities. "With HITECH there will be an increased focus on being able to conduct business in a trusted environment," said Mark Ford, principal, Security & Privacy services, Healthcare Services, at Deloitte & Touche LLP. Sixty-four percent of survey respondents indicated that they are addressing HIPAA and HITECH Act requirements, such as updating business associate agreements and updating privacy practices, to achieve meaningful use. That leaves more than a third not at that stage. For their first step, according to Ford, they should consider conducting a HIPAA security and privacy gap assessment against the updated rules to understand what needs to be fixed in order to be in compliance with the updated and expanded regulations.

As a reference point, any entity that handles ePHI in the healthcare industry could review HITRUST's (Health Information Trust Alliance) Common Security Framework, a certifiable framework for organizations that create, access, store or exchange personal health information, which Deloitte utilizes as a requirements platform to perform Meaningful Use assessment. "HITRUST is really looking to provide common set of prescriptive security requirements that allow multiple healthcare players achieve a common goal relative to their own security posture and to meet HIPAA security rule compliance," Ford said. "Furthermore, HITRUST has built its own certification program where each entity can exchange their certifications credentials as opposed to having to conduct continuous security assessments of business associates – a true 'test once and comply many' type model."

With 44 percent of respondents performing a security risk analysis of their certified EHR technology environment and 34 percent performing self-certification of their EHR technology for security and privacy requirements, healthcare providers are taking on greater responsibilities. "Certification of the individual EHR can create additional complexity because it must provide security on multiple levels and also be aligned and integrated with the healthcare organization's overall HIPAA compliance," Ford said. Healthcare providers should avoid, for example, designing a certification control that contradicts efforts of the overall HIPAA compliance program.

### **Bringing Depth and Breadth of IT and Services to Healthcare Providers**

Overwhelmed with ARRA and PPACA mandates, in conjunction with ICD-10 and 5010 conversions, many healthcare providers are seeking outside specialization to achieve compliance. Deloitte and Oracle are applying their core competencies and collaboration from their seventeen-year alliance to the healthcare industry's challenges. As a full-service professional services company, Deloitte augments its Security and Privacy practice by leveraging its various practices across its member firms, including audit and controls, systems integration, tax and financial advisory. "We look at the problem from multiple angles and help clients throughout the lifecycle by understanding the systems and bringing in the specialists, deep technology and business process experience," said Ford. Specific to healthcare, Deloitte is a certified HITRUST assessor for meaningful use, and the company's industry-focused research center, the Deloitte Center for Health Solutions, delivers additional knowledge and understanding of the healthcare industry and trends through its research and policy tracking and monitoring.

Employing a security inside-out approach, Oracle covers the entire breadth of security across the implementation and healthcare organization with its suite of comprehensive technologies. Healthcare providers can meet their specific needs with Oracle's modular, pre-integrated solutions, which comply with healthcare standards, complement other healthcare applications, are seamlessly incorporated within the clinician workflow and are flexible enough to meet future industry needs, Oakes said. By combining Deloitte's leading implementation practices and frameworks with Oracle's technologies and integration expertise, the two companies have the potential to deliver broad and deep solutions to the healthcare industry's most critical and pressing issues.

---

#### **Deloitte Statement**

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

In addition, this document contains the results of a survey conducted by a third party on behalf of Deloitte. The information obtained during the survey was taken "as is" and was not validated or confirmed by Deloitte.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this document.

Copyright © 2011 Deloitte Development LLC. All rights reserved.  
Member of Deloitte Touche Tohmatsu Limited

#### **About Oracle**

Oracle is the world's most complete, open, and integrated business software and hardware systems company. For more information about Oracle, please visit our Web site at [www.oracle.com](http://www.oracle.com).