

Balancing Practice with Compliance in Healthcare IT

An Oracle White Paper
November 2007

Balancing Practice with Compliance in Healthcare IT

OVERVIEW

Healthcare organizations today must manage two diametrically opposed sets of requirements: the practitioner's need for ease of access to information versus the business's need to apply increased privacy and security controls against that data. Establishing too much security and the organization degrades its ability to provide effective and efficient patient care; too little and the organization faces legal and civil penalties. Finding the right balance requires innovation and a strategy that continuously enhances security over time and in a layered approach.

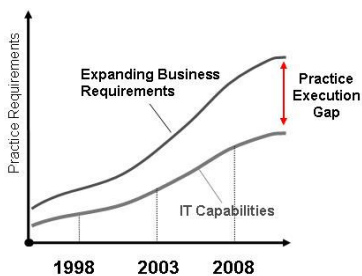
THE PRACTICE EXECUTION GAP

The "Second Annual BusinessWeek/Boston Consulting Group Survey on Innovation" (April 2006) noted that 72 percent of companies ranked innovation as one of their top three priorities. In healthcare, the need to innovate is more pronounced than in any other industry. Increasing competitive, industry, business and compliance pressures are creating new demands on provider IT infrastructures. As these business requirements continue to expand, IT infrastructure deployments and practices are being pushed to their limits. As these limits are reached, issues in leveraging them effectively become pronounced, hindering an organization's ability to innovate. This inability to innovate is represented by an ever-increasing Practice Execution Gap.

The impact of the Practice Execution Gap (PEG) on providers is evidenced in a 2006 "Healthcare Examination Study" commissioned by Oracle. The study found that only 56 percent of providers polled expressed confidence in their ability to meet the Department of Health and Human Services Electronic Health Record (EHR) implementation timeline. Of respondents, 75 percent noted IT implementation costs as the number-one obstacle to wide-scale EHR deployment, with 44 percent citing IT infrastructure challenges—calling out the need for standards and system interoperability—as major obstacles to EHR implementation. Gartner, in their most recent "IT Spending and Demand Survey" reported only 20 percent of an organization's IT budget is spent in support of new projects; the remainder, 80 percent, is spent in support of maintenance activities.

The development and deployment of new projects, such as Electronic Medical Records (EMR), Picture Archiving and Communication Systems (PACS), medication administration, materials management, practitioner and patient portals,

An organization's inability to innovate is represented by the Practice Execution Gap. Expanding business capabilities require expanding technology infrastructure. However, 80 percent of a typical organization's IT budget is allocated for support and maintenance of implemented systems with only 20 percent allocated for new projects.



“IDC believes that a new phase of identity management is emerging. This application centric approach to IAM should save organizations significant dollars in integration costs, while increasing security and providing business agility.”

—Sally Hudson, Research Manager for Security Products and Services, IDC

and master patient indexes, are all constrained by the ongoing costs of managing and supporting current IT infrastructure. Consolidating IT infrastructure services, where possible, decreases cost and complexity, freeing up resources for the evaluation and deployment of new capabilities such as those listed above.

To address these issues and minimize the PEG, organizations need to determine critical IT functionalities that exist in every application as well as their functional overlap. One such capability where function is replicated in every application is identity management. By centralizing identity management as an IT service, instead of embedding duplicate functionality in every application deployed, an organization could manage the end-to-end lifecycle of user identities across all enterprise resources.

Managing the user identity lifecycle would enable compliance and quality of care initiatives in the organization. Protected Health Information (PHI) spread across numerous clinical and enterprise systems challenges an organization’s ability to secure, audit and report on data access. Maintaining these critical data points in multiple systems with separate security roles and asynchronous privileges increases the potentiality of medical error. As organizations look to implement longitudinal patient views or collaborate with other providers, the complexity associated with best-of-breed solutions greatly increases the cost of success.

By deploying an automated identity framework, organizations can consolidate practitioner access roles and privileges, enabling quality initiatives by ensuring practitioners have access to *all* relevant data in the enterprise. The automated identity framework also enables centralized reporting and policy enforcement, decreasing time and cost associated with HIPAA, SOX, JCAHO, Gramm-Leach-Bliley (GLB) and other privacy and security compliance requirements.

REDUCING THE PRACTICE EXECUTION GAP

A Framework Approach to Identity Management

Application Centric Identity Management provides a consistent centralized framework for security policies across business applications, custom developed applications, and SOA-based Web services as opposed to embedding and managing security discretely within each application.

According to Sally Hudson, Research Manager for Security Products and Services at IDC, *“IDC believes that a new phase of identity management is emerging, which weaves the management of user identities directly into the applications themselves so that the service is part of the applications’ business processes. This application centric approach to IAM should save organizations significant dollars in integration costs, while increasing security and providing business agility.”*

The historic preference in healthcare to deliver functionality at the department level has created an environment of reaction where information technologists are limited by proprietary solutions, legacy environments and custom developed and

Application Centric Identity Management provides a consistent centralized framework for security policies across business applications, custom developed applications, and SOA-based Web services.



managed solutions that were not designed to meet ever-increasing integration demands. Many vendors today perpetuate the problem by offering niche solutions that lack end-to-end capability or do not support standards, thereby hindering an organization’s ability to integrate across the enterprise. Integration problems are typically compounded as organizations deploy point solutions such as single sign-on, clinical context management through Clinical Context Object Workgroup (CCOW) integration, Lightweight Directory Access Protocol (LDAP) or directory services, password management and advanced authentication services, in an attempt to address a departmental requirement. Without an integrated framework to base these technologies on, the business value and success of these projects remains limited.

Oracle has developed three solutions directed at the needs of healthcare providers: *Provider Experience Management*, *Enterprise Role and Identity Management for Healthcare* and *Auditors Warehouse for Healthcare*. All three solutions are based on Oracle’s Identity Services Framework, a standards-based identity management infrastructure capable of being leveraged by third party ISV applications, Oracle Fusion applications and middleware, custom developed applications and legacy applications running in an enterprise.

Oracle has developed three solutions directed at the needs of Healthcare Providers: *Provider Experience Management*, *Enterprise Role and Identity Management for Healthcare* and *Auditors Warehouse for Healthcare*.



Provider Experience Management

Industry averages today show a typical physician spends approximately seven minutes per patient encounter, of which he or she spends up to two minutes on IT tasks including managing logins and passwords and application navigation. As new systems are brought online, which require additional credentials to login, the impact on the provider increases—leading to further reductions in time the provider spends with patients. Tasking the provider with an ever-increasing list of IT related tasks ultimately leads to fewer patient encounters.

The challenge for healthcare organizations is to create an environment that simplifies access to core clinical data sets while maximizing the time providers can interact with patients without jeopardizing data integrity and security. Simplifying this experience helps increase quality of care by enabling the provider with a more complete view of patient data and decreasing time and effort spent at the console gathering the data.

Practitioners typically work with many healthcare organizations in their regions through physicians groups, specialist or contract nursing organizations. Studies show that organizations focused on simplifying the provider experience become the provider’s preferred organization. Ultimately, this results in increased mind share with providers and revenue potential for the organization.

Experience Simplification

To simplify the provider experience, organizations need to bring the concept of multi-faceted identity based services to the end user level. Many organizations have undertaken “phase1” project initiatives, such as enterprise single sign-on,

context management or advanced authentication, to simplify the provider experience. These initiatives, however, have not met provider expectations because they do not address the entire problem that providers experience. Answering to the entire problem requires an enterprise approach that encompasses enterprise single sign-on, context management, advanced authentication and the ability to deliver fast, efficient workflow to manage the user experience.

According to META Group research, on average, internal user information is stored in 22 distinct data stores while external user information resides in six distinct data stores across a typical enterprise.

Enterprise Single Sign-On (eSSO)

An enterprise single sign-on service must integrate not only with clinical systems, but also with critical network and infrastructure components such as email, file sharing and enterprise collaboration services. Enterprise single sign-on improves the user experience when accessing multiple applications, but it only provides the initial authentication to the system. To truly impact the experience, an organization must also provide context management.

Context Management (CCOW)

The promise of CCOW is enormous but, in practice, it is limited by the organization's ability to upgrade to CCOW compliant versions of their critical applications. Because most organizations cannot wholesale upgrade applications across the enterprise in support of a CCOW initiative, a better approach would be to integrate applications through single sign-on and provide context management when the provider accesses a system that supports it. The initial benefit the provider experiences through single sign-on and password management will allow corporate IT the opportunity to investigate integrating non-CCOW compliant applications.

Advanced Authentication for Simplification

Advanced authentication has typically been viewed as an enterprise security solution and rarely evaluated as a means to simplify the provider experience. Advanced authentication provides for a single authentication mechanism, reducing the user's need to manage numerous access methods, credentials and passwords. To support layered security at the enterprise level, many organizations implement multiple authentication capabilities such as active and passive proximity, biometric and tokens so that the right method can be selected for the right departmental application. With Advanced authentication, each of these methods can be leveraged and still provide for a simplified provider experience.

Advanced Workflow Support

Simple technology-only solutions force changes to the way providers manage their patient flows or clinical presence. In order to gain the most benefit from the technology, however, the solution needs to be flexible enough to drive simplification without dramatically changing or re-architecting user expectations or workflows.

Oracle's Provider Experience Management is an enterprise class solution that directly addresses provider experience simplification and increases provider patient contact per encounter. By leveraging a solution that integrates enterprise single sign-on, advanced authentication and context management from one of the industry's top vendors, an organization can provide access to the right data in less time—increasing quality of care and provider satisfaction within the organization.

A Gartner Research report, "Focus on Human Resources Applications," predicts that automated on-boarding tools that bridge the recruitment and retention processes are critical to successful talent retention. "Self-service is taking off as HR organizations aggressively pursue coordinated techniques for delivering information, benefits, forms and context through corporate intranets and other electronic channels."

- Diane Morello, Vice President and Research Director, Gartner

Enterprise Role Management for Healthcare

Healthcare organizations today utilize numerous methods to staff the business, including contract nursing, physicians and specialist groups. As onsite staff, even though they may not be in the HR system, staff privileges and levels of authority must be maintained in a system of record. In most healthcare organizations, the automation of user privileges ends at the HR system. Granting appropriate access to the enterprise systems and applications required for the individual to perform his or her duties is a manual and time consuming process; this process often leads to a significant amount of "down time" where the user is onsite but not yet provisioned appropriately. An additional challenge encountered with manual provisioning is the possibility of granting incorrect permissions to an individual. If an error occurs due to manual mis-provisioning, the organization often times is unaware until an audit reveals the infraction.

When a new user joins a department, the hiring manager typically requests access to IT systems through help-desk work orders, email requests, or by making phone calls. The level of access requested can vary widely depending on the person's role or responsibility within the department. Most often the manager will simply request that the new employee be granted the same privilege as another team member who performs a similar role. This method breaks down, however, as people are transferred and promoted in the organization. If the second hiring manager performs the same diligence as the first, then the user will end up with an aggregate privilege representative of their previous and current roles. The less often the organization performs attestation, reviewing each user's appropriate versus configured privilege, the higher the potential for a user to have inappropriately authorized access and the higher the organization's risk of exposure.

To address this issue organizations must determine how often attestation should occur. User access audit responsibilities in response to HIPAA, JCAHO, SOX, and other mandates require significant time and effort to accomplish due to the nature of this commonly utilized manual provisioning model. Ad hoc reporting capabilities for point in time validation are hard to deliver and do not necessarily mitigate risk because they are only valid the instant the report is run.

Oracle's Enterprise Role Management for Healthcare, an automated, role-based provisioning solution, addresses both the issues of manual mis-provisioning and inappropriately aggregated privilege. As users change roles or user roles change, individual privileges are automatically appended or deprecated to reflect the new responsibilities. Because the provisioning process is workflow driven, approval and

denial of access is logged for audit. When users leave the organization or their access is no longer required or valid, user access can be revoked through a one button de-provisioning process that terminates the user's access across all managed resources, eliminating a common security risk.

In *Maximizing Returns on Recruiting Investments: Identifying Drivers of Internal Transfer Performance*, Brian Kropp, Ph.D. and Senior Consultant, Recruiting Roundtable states, "Onboarding is the most critical part of the internal hiring process. Most organizations have focused their onboarding efforts on external hires, but this research clearly demonstrates that such a stance is not sufficient. Similar to externally hired employees, internally transferred hires require targeted onboarding to help them succeed in their new job."

Oracle Enterprise Role Management for Healthcare uses a uniquely powerful and flexible framework comprised of Organizational Roles, IT Roles and Approver Roles. Role governance and administration can be delegated by policy to allow the right people to make the right access decisions. The entire process is managed through a configurable, easy-to-use user interface that gives users and IT personnel the tools to manage privileges efficiently and effectively in support of governance initiatives.

Healthcare organizations are in constant flux, making the task of granting appropriate and timely access to information a critical challenge. Organizations that are able to provide the appropriate data and enterprise access quickly, reliably and securely will benefit from reduced cost and risk. By establishing an authoritative source for enterprise roles, an organization will be better able to meet governance and compliance needs across the entire enterprise.

By leveraging a single point of policy management, organizations can maintain and manage roles, role membership and associated access privileges all from a single source, enabling consistent enforcement of rules across the enterprise. As the organization evolves, users are automatically provisioned, or de-provisioned, based on these rules so that user privilege remains aligned with the business practice.

Oracle Enterprise Role Management for Healthcare also allows users to manage the operation of their organization. End users, managers and administrators can track request status in real time, at any point during the provisioning process. This allows the organization to maintain better control over and improve visibility into the privilege assignment process.

Approval workflows are also logged to enable alignment with an organization's governance, risk, and compliance (GRC) initiatives. Managers need only attest to rules and to whom these rules apply, instead of tens of thousands of individual privilege combinations—freeing them to focus on their core responsibilities. This centralized, comprehensive view of people, roles and privilege, results in more accurate and efficient auditing and reporting and allows continuous review and improvement of policies and controls.

Organizations that implement role management at an enterprise level find that assigning privilege based on role appears trivial compared to defining and determining the set of enterprise roles. Oracle Enterprise Role Management for Healthcare assists in the development of roles by uncovering roles currently utilized in enterprise and clinical systems and aggregating the policies used to govern these roles. The system utilizes sophisticated statistical analysis to determine user and privilege relationships; then, the system clusters these relationships into candidate roles and presents the roles in an easy-to-understand

graphical relationship hierarchy. Additionally, users can refine role definitions and perform impact analysis, and users can generate reports for broader review and validation. Finally, users can export verified roles, business rules and access policies into the role management system for complete and automated role life-cycle management.

Many historical attempts at enterprise provisioning have failed due to the inability of the provisioning tool to link to the organization's primary systems. The Adapter Factory®, a component of the Oracle Enterprise Role Management for Healthcare solution, eliminates the complexity associated with creating and maintaining the connections and complements the large collection of system connectors available out of the box. The Adapter Factory provides rapid integration to commercial or custom systems without programming. Once created, connectors are managed within the provisioning system, making extending, maintaining and updating connections a manageable and straightforward process.

Oracle Enterprise Role Management for Healthcare is an enterprise-class system of record for managing relationships, roles and related resources. Healthcare organizations can now capture, model and update relationships between people, processes, projects, documents, locations and resources, enabling them to operate in real-time and effectively meet increasingly complex compliance requirements.

Auditors Warehouse for Healthcare

Healthcare organizations today face an ever increasing challenge in meeting compliance objectives leveled by numerous governmental agencies, industry watch certification groups and the threat from patient safety and privacy advocacy groups. In order to meet these challenges, organizations must be able to certify that users accessing patient health data are privileged to do so as a matter of clinical practice. The cost and complexity of these enterprise wide certifications can be astounding. And, the diverse audit services within enterprise and clinical systems as well as different access mechanics for data make it nearly impossible to develop a consistent end to end audit trail for end user activity. Because they lack the ability to programmatically validate administrative user activities, many organizations simply *trust* administrative users not to access data in ways inconsistent with enterprise security policy.

Satisfying compliance regulations and mitigating the risks associated with insider threats are two of the top security challenges healthcare payers and providers face today. Oracle Auditors Warehouse for Healthcare reduces the cost and complexity of compliance and the risk of insider threat by automating the collection and consolidation of audit data. This solution provides a secure and highly scalable audit warehouse, enabling simplified reporting, analysis, and threat detection on audit data. In addition, database audit settings are centrally managed and monitored from within Auditors Warehouse, reducing IT security costs.

Satisfying compliance regulations and mitigating the risks associated with insider threats are two of the top security challenges healthcare payers and providers face today. Oracle Auditors Warehouse for Healthcare reduces the cost and complexity of compliance and the risk of insider threat by automating the collection and consolidation of audit data.

In *What CFOs should know—and do—about corporate responsibility*, published in *Healthcare Financial Management*, James R Schwartz states, “Many of the public-policy considerations inherent in Sarbanes-Oxley will spill over onto not-for-profit corporations—health care organizations in particular. The fundamental policy concern, preservation of the integrity of a corporation's financial statements, transcends the basic distinctions between publicly traded corporations and not-for-profit corporations.”

The results of a 2007 survey of Sarbanes-Oxley costs conducted by Foley & Lardner LLP and published in the November 19, 2007 issue of *LegalTimes*¹ showed that the average cost of compliance with the Sarbanes-Oxley act more than doubled between the initial year of SOX compliance and 2006 for companies with under \$1 billion in annual revenue. According to the study, in the last year alone, related expenses rose 13 percent with 4 percent being attributed to the external audit itself. The report found that audit fees alone now represent more than 47 percent of out-of-pocket corporate governance compliance costs for companies with less than \$1 billion in annual revenue.

HIPAA, JCAHO, Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Basel II and various regional privacy directives are just a few of the regulations and industry standards healthcare organizations face in today's global business environment. Organizations not only have to protect sensitive information, but they also need to monitor access to sensitive information for compliance and to guard against potential threats. Examination of numerous insider crimes has shown that had there been an effective auditing system in place, the resulting financial impact would have been reduced substantially. Leveraging audit data to minimize this impact, however, has proven to be difficult due to the distributed nature of audit data which makes analysis, reporting, and alerting difficult.

Oracle Auditors Warehouse for Healthcare transparently collects and consolidates audit data, providing valuable insight into who did what to which data when—including privileged users who have direct access to the database. With Oracle Auditors Warehouse for Healthcare reports, alert notifications, and centralized audit policy management, an organization greatly reduces its risks from internal threat as well as the cost of compliance. Oracle Auditors Warehouse for Healthcare leverages Oracle's industry leading database security and data warehousing technology for managing, analyzing, storing, and archiving large volumes of audit data.

Oracle Auditors Warehouse collects database audit data from audit trails in the database and on the operating system. Additionally, it can also read the transaction logs to capture the before and after values associated with transactions. Oracle Auditors Warehouse supports Oracle9i Database Release 2, Oracle Database 10g Release 1 and Oracle Database 10g Release 2. Future releases will include the ability to collect audit data from non-Oracle databases sources and build custom audit collectors for other sources.

¹Hartman, Thomas E. (2007, November 19). How Much for SOX? *LegalTimes*.

Retrieved November 16, 2007, from

http://www.foley.com/files/tbl_s31Publications/FileUpload137/4588/HartmanSOX_Nov19_2007.pdf

The first audit of HIPAA security compliance was conducted by HHS earlier this year. According to Barry Runyon, an analyst at Gartner, “There are going to be more feet on the street from HHS going on unannounced audits.”

Oracle Auditors Warehouse for Healthcare provides: standard audit assessment reports covering privileged users; account management; roles and privileges; and object management and system management across the enterprise. An organization can define parameter driven reports showing user login activity across multiple systems and within specific time periods, such as weekends. The open audit warehouse schema can be accessed from Oracle BI Publisher, Oracle Application Express or any third party reporting tool.

Oracle Auditors Warehouse for Healthcare event alerts help mitigate risk and protect from insider threats by providing proactive notification of suspicious activity across the enterprise. Additionally, Oracle Auditors Warehouse continuously monitors the inbound audit data, evaluating audit data against alert conditions. And, alerts can be associated with any auditable database event including system events such as changes to application tables, role grants, and privileged user creation on sensitive systems. Finally, Oracle Auditors Warehouse provides graphical summaries of activities causing alerts.

Protecting audit data is critical to the security and internal controls processes. Oracle Auditors Warehouse protects audit data by using sophisticated controls including Oracle Database Vault and Oracle Advanced Security. Access to the audit data within Oracle Auditors Warehouse is strictly controlled. Privileged DBA users cannot view or modify the audit data and even auditors are prevented from modifying the audit data.

Oracle Auditors Warehouse leverages Oracle’s proven data warehousing and partitioning capabilities to achieve massive scalability, a key requirement for any auditing solution. Oracle Auditors Warehouse can optionally be deployed with Oracle Real Application Clusters (RAC), enabling scalability, high availability, and flexibility.

Further, with Oracle Auditors Warehouse, IT security personnel work with auditors to define audit settings on databases and other systems across the enterprise to meet both compliance requirements and internal security policies. Oracle Auditors Warehouse provides the ability to provision and review audit settings in multiple databases from a central console, reducing the cost and complexity of managing audit settings across the enterprise.

Addressing regulatory compliance requirements and protecting against insider threats in today’s Healthcare environment requires a defense-in-depth approach to security. Oracle Auditors Warehouse automates the consolidation and analysis process, turning audit data into a key security resource to help address today’s security and compliance challenges.

CONCLUSION

Managing the practitioner's need for ease of access to information versus the business's need to apply increased privacy and security controls against that data is becoming more difficult as organizations implement new systems, capabilities and products to serve their communities.

Finding the right balance between provider enablement and data security requires innovation and a strategy that continuously enhances security over time and in a layered approach. Oracle's Identity Management solutions for Healthcare help diverse healthcare organizations manage that balance by enabling increased organizational innovation and agility and better decision-making while reducing the cost and risk associated with compliance initiatives.



Balancing Practice With Compliance in Healthcare IT
November 2007

Authors: Robert Batterton, Reid Oakes
Contributing Author: John Carlson

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Copyright © 2007, Oracle Corporation and/or its affiliates. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.