An Oracle White Paper
October 2011

HITECH's Challenge to the Health Care Industry

Introduction

The Health Information Technology for Economic and Clinical Health Act (HITECH) forces health care providers and their business associates to bring a sense of urgency to the security of protected health information (PHI). The act brings both pressures and incentives into play in its mandate to convert PHI to electronic health records (EHR), and puts teeth into the enforcement of the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA).

Although the HIPAA Security and Privacy rules have been in effect since 2003, auditing has been, at best, spotty, enforcement and imposition of penalties rare, and they did not apply directly to business associates. Under these conditions, it's not surprising that healthcare has lagged behind most other industries in their security programs.

More than one fifth of the respondents in the 2009 survey conducted by the Healthcare Information and Management Systems Society (HIMSS) reported that security accounted for less than 1% of their budget, with almost no change from the previous year. Forrester Research's annual security survey showed that healthcare trails financial services, retail and government sectors in the percentage of overall IT budget spent on security.

Information security has not been a high-priority issue for hospitals, which naturally evaluate commitment of energy, spending and allocation of resources in terms of their impact on the quality of patient care. Before HITECH, there were no incentives and little concern about enforcement.

Conversion to EHR will result in explosive growth in digital information sharing among health information exchanges, hospitals, medical practices and business associates. Under HITECH, all recipients of PHI contained in EHR are now subject to the same requirements for protecting PHI. The risk of inadvertent or malicious disclosure of health information increases dramatically, and there is evidence that attackers are taking note and targeting healthcare institutions in growing numbers.

In this environment, healthcare providers should assess their security programs and ensure that they have the policies, processes and supporting automated tools in place to protect patient information.

HITECH Changes the Game

The Move to Electronic Health Records (EHR)

The HITECH Act is part of the $787 billion American Recovery and Reinvestment Act (ARRA), more commonly known as the Stimulus Bill, enacted in February 2009. The core purpose of HITECH is to convert the nation's health care records to digital formats, improving health care through the rapid transmission of medical information and ultimately saving money on operations by making the nation's health care systems more efficient.

HITECH takes a carrot-and-stick approach to promote the mandated conversion to EHR. The act provides $19.2 billion to promote the conversion, most of it going to Medicare and Medicaid reimbursement as incentives to make what the act refers to as "meaningful use" of EHR, starting in 2011. The stick comes in the form of reduced reimbursement, starting in 2015, for entities that do not use EHR.

But the really hard end of the stick is how HITECH, recognizing the increased risk of electronic PHI, ups the ante for healthcare providers and their business associates who fail to meet the HIPAA Security and Privacy Rules requirements.

Increased Penalties

Previously, penalties could be assessed at $100 per violation, capped at $25,000 per year for multiple violations of an identical requirement or prohibition. HITECH sets the range at $100 up to $50,000 per violation, capped at $1.5 million per year for multiple violations of an identical requirement or prohibition.

Moreover, individuals, such as hospital employees, in addition to covered entities, can be held criminally liable with fines of up to $250,000 and up to 10 years in prison for HIPAA violations. In addition, if the Department of Justice declines to prosecute, the Department of Health and Human Services Office of Civil Rights (OCR) can still bring civil suit. A percentage of the civil penalties collected are distributed to individuals affected by the violations.

More Aggressive Oversight

Beyond any promises of greater oversight and more aggressive enforcement, both federal and state governments now have incentives to investigate possible violations and file suit when the evidence is sufficient. Under HITECH, money collected in civil penalties is funneled back into OCR's enforcement budget. The act also permits state attorneys general to bring civil actions against HIPAA violations, making wider oversight and enforcement far more likely. In January, for example, Connecticut Attorney General Richard Blumenthal sued Health Net of Connecticut, alleging the company violated HIPAA when it lost a portable disk drive containing health and financial information of about 446,000 enrollees. The action claimed that Health Net did not properly secure the information and failed to notify consumers of the security breach.

Breach notification

HITECH mandates data breach notification, putting pressure on providers to avoid the costs and negative public exposure associated with data breaches involving PHI.

The requirement is similar to the 40-plus state data breach notification laws, which cover exposure of consumer information. These laws typically exempt encrypted information, assuming that it cannot be read by anyone who obtains possession. HITECH states that breach notification applies to "unsecured PHI," defining unsecured as information that has not been rendered "unreadable, unusable or indecipherable" to unauthorized individuals. In practical terms, HHS guidance means encrypting the data or destroying it.

The act requires the health care provider to notify the affected individuals of the breach, as well as the Department of Health and Human Services (HHS) if 500 or more patients are affected. HHS posts these breaches on its Web site. Violators must also notify prominent media if the breach affects more than 500 people in a particular location.

Business associates, now subject to HIPAA Security Rule requirements, must notify their covered entity partner if they are responsible for or victim of a PHI breach.

It's important to note that HITECH does not *require* encryption (it makes encryption an "addressable" controls rather than a "required" one). However, as with the state laws, encryption generally obviates the need for breach notification.

As HHS points out in its guidance, using encryption does not change the Security requirements to protect PHI. Encryption is only one step in support of a holistic security program that includes data protection, identity and access management policies, enabled and supported by the right tools. Today's health care information environment, involving many disparate organizations, and many people performing different roles, and communicating in multiple ways, doesn't lend itself to a simplistic security solution.

HITECH's Challenge

The Health Care Risk Environment

The modern healthcare information environment is complex, with information flowing across numerous interrelated and interdependent institutions, service providers and individuals: Physicians inside the hospital and at their practices, outsourced diagnostic services, pharmacies, labs, billing services, business associates, visiting nurses and other home/mobile healthcare providers, rehab centers, clinics, etc.

Electronic patient information is communicated not only via LAN and WAN but all forms of wireless devices, from laptops to smart phones to specialized handheld medical information devices.

The challenges are daunting. Covered entities and business partners must consider several factors, including:

- Identifying the information that is considered PHI under statute and carries the risk of harm to the patient and non-compliance to the organization.
- Balancing the need to protect information from exposure while still providing the highest level of patient care.
- Extending information access and policy enforcement beyond the organization to the myriad of partners, service providers and suppliers that support the health care provider.
- Identifying the applications that have access to PHI, validating whether that access is appropriate, as well as the individuals, groups and organizations authorized to use those applications, with appropriate limitations.

Develop a Holistic Security program

In this environment, health care providers must think and act in terms of a comprehensive information security program that incorporates protection around the data to prevent its use by unauthorized individuals. This includes creating and implementing granular, role-based, access control, authorization and authentication policies that help ensure that health information is properly secured and health care providers are compliant.

Health care organizations must:

- Identify, classify and assess risk around data.
- Implement appropriate protection, such as strong encryption and data masking to prevent unauthorized exposure and at worst, malicious use.

- Assign the appropriate privileged user roles, with careful attention to maintaining separation of duties.
- Monitor data access, with particular attention to the activities of privileged users, such as database administrators.
- Establish individual and group roles, evaluating and adapting them as needs change.
- Create policies and workflow processes with clear responsibilities and accountability for provisioning and de-provisioning users, approving job changes, as well as application, information and systems access authorization.
- Implement logging, audit and reporting capabilities around application and data access, administrative functions; user and asset access activity, provisioning and de-provisioning.

The Security and Compliance Burden

Managing and maintaining this type of program in a dynamic environment is a heavy burden for health care organizations dedicated to devoting maximum resources and focus on the quality of patient care. Personnel come and go; patients are discharged; business partner relationships change; new applications and systems come online, and new services become available.

Oracle database security and identity management products provide a complete single-vendor defense-in-depth security strategy that can help customers address a broad set of requirements.

Consider the difficulties of translating this into a manageable, efficient security and compliance program.

The Data Protection Challenge

Retrofitting existing applications with strong data protection can be a time consuming, costly, and seemingly impossible exercise. After all, most applications running today along with their supporting infrastructure were built for high availability, scalability and usability. In most cases, the data security that does exist resides solely in the application layer and consists of a username and password along with a mapping of users to various roles and responsibilities within the application, thus limiting access to application screens and functions. Outside the context of the application, data remains unprotected and vulnerable to application bypass attacks. Information security in terms of encryption, masking, access control and monitoring remains a relatively specialized area that only recently has seen technology progress to the point that it can be widely adopted by those with little to no security background and applied to existing applications without costly and time-consuming changes.

Take for example data encryption and the associated key management requirements. Encryption algorithms have been widely available for well over a decade. The ability, however, to apply encryption technology to practical business problems, as required by HITECH, has been limited.

This was due to the changes, both technical and administrative, required to deploy encryption. Encryption needs to be transparent to existing applications, non-disruptive to the existing high availability strategy and be easy to administer in a large, distributed environment. Similarly, deploying additional access controls on data outside the application layer without breaking the application was viewed as next to impossible. In fact, access to application data by administrative personnel operating outside the application has to this point been considered the norm.

Thus far, separation of duty enforcement along with deployment of preventive controls on access to application data by administrators operating outside the application has been considered too operationally disruptive. In addition, the increasingly important task of monitoring audit logs for unauthorized or inappropriate activity has languished due to the time consuming, resource intensive nature of the task. This is despite numerous examples where such monitoring would have greatly reduced or even prevented unauthorized disclosure of sensitive information.

Oracle's comprehensive database security portfolio, including *Oracle Advanced Security*, *Oracle Data Masking*, *Oracle Database Vault* and *Oracle Audit Vault,* protects information by providing transparent data encryption, masking, privileged user and multi-factor access control, row level data classification, as well as continuous monitoring of database activity.

The Access Control Challenge

Maintaining an effective access control program is even more challenging, as the health care provider typically must administer authorization and appropriate authentication on a per-application basis. It's impossible to administer and enforce unified policy across applications and systems; management is fragmented and laborious, policy inconsistently applied and users frustrated.

Policy-based provisioning and de-provisioning of user access and authorization is:

- Fragmented by reliance on each application
- Hampered by a lack of an automated workflow to assure that authorization is appropriate and approved by the responsible managers, who can be held accountable for their action.
- Reliant on group-based authorization, which can be too coarse for fine-grained controls, making provisioning an inexact science that typically leads to too much privilege, which is a security risk, rather than too little, which impedes work and ultimately, would impact patient care.

Monitoring user access activity for malicious behavior and policy violations and producing auditable reports and responding to auditor requests will be manual and error prone, and difficult to coordinate. Administrators have to collect and query access logs, for example, from diverse applications, *if* they are available.

Further, health care providers have to extend special sets of access control rules to numerous third parties who need to access or share PHI. Assigning and administering access controls outside the core organization is exceedingly difficult. Great care has to be taken to assure that the disclosure of PHI is the minimum needed to perform the contracted services, but easy and manageable enough to allow critical medical information to move without delay.

Oracle Access Manager, *Oracle Identity Manager, Oracle Identity Analytics, Oracle Identity Federation* and other products in the suite of Oracle identity management solutions provide application and system-level security, enabling health care organizations to create and sustain a centrally managed, automated and auditable access control program.

Frameworks for Compliance

Standards-based Controls

In addition to the specific Privacy and Security controls required by HIPAA/HITECH, it's highly recommended that health care organizations look to one or more of the accepted control standards, such as ISO27002, NIST and COBIT, as the foundation of their HIPAA/HITECH security and compliance programs. As organizations move to electronic health records, they must implement required controls around the maintenance and flow of health information. This will enable organizations to capture HITECH incentive reimbursement, avoid penalties, protect themselves against the heightened oversight from HHS and state attorneys general and guard against the damage of a major PHI breach and the negative impact of the required notification.

A standards-based approach:

- Provides a well-defined set of controls that can serve as a template to be modified to the organization's special requirements as a member of the health care industry.
- Provides a yardstick for the organization to measure progress and evaluate its security program.
- Demonstrates to auditors that the organization is following a well-conceived initiative that follows universally accepted control recommendations.
- Forms a common basis for establishing security controls and trust across entities to assure that PHI is being transmitted and maintained as it is shared across organizations.

Role of Business Associates

The last point emphasizes the need to maintain strong controls as information is shared outside the provider organization. The HIPAA Security Rule has always required health care providers to have contracts that direct business associates to safeguard PHI. However, now that HITECH puts the same security requirements on business associates as for covered entities, those contracts will need to be modified to reflect these new obligations.

HITECH expanded the definition of a business associate to include organizations that transmit and routinely access PHI, such as health information exchange organizations, regional health information organizations and vendors. Previously, business associates were liable only under the terms of their contracts, but under HITECH, they are subject to direct government oversight and civil and criminal penalties for HIPAA violations.

HITRUST's Common Security Framework

The Health Information Trust Alliance (HITRUST) has addressed these issues with a health care industry-centric approach to standardize security controls and streamline compliance programs. The Common Security Framework (CSF) incorporates hundreds of IT controls from other frameworks that are relevant to the health care industry, such as NIST, ISO, COBIT, HIPAA/HITECH, PCI DSS and SOX.

The CSF contains 13 security categories encompassing 42 control objectives and 135 control specifications.

It is too early to tell if HITRUST will become a widely embraced standard for HIPAA/HITECH and other regulations that impact the health care industry, but it is well worth considering as the basis for a security/compliance program and a common ground for meeting contractual obligations.

HIPAA SECURITY RULE		ORACLE PRODUCTS AND FUNCTIONALITY THAT HELP ADDRESS HIPAA SECURITY RULE REQUIREMENTS
164.308 Administrative safeguards		
(a)(1)(ii)(A)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Oracle Change Management discovery, asset tracking, change detection, compliance assessments
(a)(1)(ii) (D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	• Oracle Audit Vault database monitoring and reporting, secure repository • Oracle Database Vault auditing and reporting on access attempts, etc. • Oracle Access Manager user access activity logs and reporting • Oracle Identity Manager user identity information audit and reports
(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected	• Oracle Database Vault privileged user controls: access realms and command rules, separation of duties • Oracle Identity Manager user and user authorization

HIPAA SECURITY RULE		ORACLE PRODUCTS AND FUNCTIONALITY THAT HELP ADDRESS HIPAA SECURITY RULE REQUIREMENTS
	health information and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.	provisioning • Oracle Access Manager automated, centralized access control • Oracle Identity Analytics role management • Oracle Identity Federation
(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information	• Oracle Database Vault privileged account authorization, separation of duties • Oracle Access Manager centralized access control and authorization • Oracle Identity Manager user authorization provisioning • Oracle Identity Federation
(a)(3)(ii)(A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	• Oracle Database Vault • Oracle Identity Manager • Oracle Identity Analytics • Oracle Access Manager • Oracle Identity Federation
(a)(3)(ii)(C)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in [above]	Oracle Identity Manager automated de-provisioning of terminated users, inactive accounts and obsolete authorization. "Rogue" account detection
(a)(4)(i)(B)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	• Oracle Database Vault • Oracle Access Manager • Oracle Identity Manager
(a)(4)(i)(C)	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	• Oracle Database Vault • Oracle Access Manager • Oracle Identity Manager
(a)(5)(i)(C)	Implement procedures for monitoring log-in attempts and reporting discrepancies.	• Oracle Audit Vault • Oracle Database Vault • Oracle Access Manager
(a)(6)(ii)	Identify and respond to suspected or known security incidents	• Oracle Audit Vault monitoring and alerting • Oracle Access Manager monitoring and alerting • Oracle Identity Manager rogue account detection
164.312 Technical safeguards		

HIPAA SECURITY RULE		ORACLE PRODUCTS AND FUNCTIONALITY THAT HELP ADDRESS HIPAA SECURITY RULE REQUIREMENTS
(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights	• Oracle Database Vault privileged account management and separation of duties • Oracle Access Manager access control, authorization and authentication • Oracle Identity Manager user authorization provisioning • Oracle Identity Analytics role management
(a)(2)(i)	Assign a unique name and/or number for identifying and tracking user identity.	• Oracle Database Vault • Oracle Identity Management
(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	• Oracle Identity Management facilitates dynamic provisioning for urgent business needs and de-provisioning when the need passes
(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	• Oracle Advanced Security transparent data encryption (TDE) provides transparent encryption of stored data and built-in cryptography key management
(b)	Audit controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information	• Oracle Audit Vault • Oracle Database Vault • Oracle Access Manager • Oracle Identity Manager
(c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	• Oracle Database Vault privileged account management and separation of duties controls access and authorization to PHI • Oracle Access Manager access control, authorization and authentication
(d)	Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	• Oracle Database Vault authentication command rules • Oracle Access Manager support for multi-factor authentication
(e)(1)	Transmission security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Oracle Advanced Security provides SSL/TLS support for encrypted transmission and strong authentication via Kerberos, RADIUS and PKI
(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Oracle Advanced Security encryption and authentication
(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Oracle Advanced Security

Comprehensive Data Security

Defense-in-Depth

Oracle is an established leader in protecting information stored within databases and delivers security features and solutions to assist health care customers in securing PHI. In addition to providing high availability and massive scalability to support the continuous flow of PHI vital to patient treatment and timely delivery of critical services, Oracle data security solutions enforce security controls where the data resides, including principles such as need-to-know, least privilege, and separation of duty.

Oracle provides strong controls on privileged user access to application data. Privileged users have the ability to maintain the database, reflecting the minimum access required to do their jobs, but generally should not be allowed to see or manipulate critical data. This is essential in a health care environment, in which patient information should be disclosed only on a need to know basis for medical treatment and essential support services.

Oracle's defense-in-depth suite of database security solutions help health care providers and business associates implement and manage a best-performer data security program.

Defense-in-depth data security means looking at data security holistically. To do that, one needs to look at the entire life cycle of the data, where the data resides, what applications access the data, who is accessing the data and under what conditions, and ensuring that the systems have been properly configured and remain that way. Key elements of this approach include encryption and data masking, access control, and monitoring.

Access controls beyond the application level are now vital to enabling organizations to achieve the benefits of data consolidation, off-shoring and cloud computing. Historically, applications have been designed to scale to Internet requirements and provide role based functional access. Today, however, regulations and privacy laws require limited access to application data, even by the database administrator and especially from ad-hoc tools that can be used to bypass the application.

While encryption and access control are key components to protecting data, even the best security systems are not complete without a monitoring system in place. Just as video cameras supplement audible alarms in homes and businesses, monitoring provides the corresponding who, what and when that complements the encryption, masking and access control systems.

How Oracle Protects Patient Information

Data Encryption and Masking

Classification of data — in this case, most importantly, PHI — is a strong determining factor in applying the appropriate level of protection required across the board. While PHI distribution and disclosure must be limited by strong access controls, it must be made quickly and transparently available to health care practitioners and supporting service providers as needed. This means protecting the data beyond the access controls within the database and restricting direct access at the underlying operating system.

Encryption is essential to protect data from unauthorized use, whether it is on disk underneath the database and applications, in development environments, in transmission or on backup media.

Oracle Advanced Security transparently encrypts data when written to disk and decrypts it after a user has been successfully authenticated and authorized. This is provided by the *Oracle Advanced Security transparent data encryption (TDE)* capability. TDE supports table column encryption and tablespace encryption. TDE prevents attempts to bypass the database and access files directly either at the operating system layer or on backup media. TDE tablespace encryption is fully integrated with *Oracle Advanced Compression*, enabling organizations to leverage encryption and reduce storage requirements. *Oracle Advanced Security* is consistent with the HITECH guidance for strong encryption algorithms supporting AES (256, 192 and 128 bits) and 3DES (3 and 2 keys; 168 bits).

Data encrypted with TDE remains encrypted on backup media without any modification to existing backup procedures. In addition, TDE is integrated with Oracle Data Pump, enabling data extracted from the Oracle database and written to a flat file, to be encrypted.

Oracle Advanced Security also provides network encryption and strong authentication services. It can be used to enable SSL/TLS encryption to protect data going to and from the database as well as enforces strong authentication to the Oracle database using Kerberos, PKI or RADIUS.

Data masking is another essential tool in protecting PHI against improper use, consistent with the HITECH concept of limited disclosure. Under HITECH, health care providers and business associates must limit PHI use to the minimum necessary to accomplish the required purpose.

Oracle Data Masking replaces sensitive information, such as social security numbers or other personal identifiers, with faux values in the same format, allowing PHI to be used for development, testing, and research in which de-identified data is sufficient so that the information is not associated with an individual.

Database Enforced Access Controls

Privileged users, such as administrators with elevated rights, are often overlooked as security risks, yet they typically have the highest level of access and authorization, often to information that is not required to perform their duties. In a health care context, this means they may well be able to read, copy, or even alter PHI. Because of this, hackers and organized crime organizations may target privileged users' authentication credentials as a means of accessing PHI. Ironically, privileged users, who have the most potential to do harm, inadvertently or intentionally, are the most poorly managed in terms of access control, due to concerns over disrupting operations.

Oracle Database Vault provides strong privileged user access control, using the concept of "realms" to create a firewall within the database. Sensitive tables or applications can be placed in a realm, so privileged users can do their jobs without having access to PHI or other sensitive data. So, for example, a DBA can perform his job without being able to see patient medical and/or personally identifiable information in an application. *Oracle Database Vault* granular security rules can employ multiple factors such as IP address, time of day and authentication method to enforce policies over who, when, where and how PHI data should be accessed, creating a "trusted-path" to the PHI data and ensuring the ad hoc tools downloaded from the Internet cannot be used to bypass the approved application.

Monitoring, Alerting and Reporting

HITECH raises the specter of increased audit and investigatory oversight at both the federal and state levels. Health care providers need to be prepared to present audit reports, respond to queries and government investigation quickly with proof that controls are more than paper policies. Holistic security should demonstrate not only a snapshot of information oversight at any given point in time, but reflect continuous monitoring of all database activities and alerting of possible anomalous transactions.

However, preparing for and responding to audits is typically labor intensive, expensive and error prone, requiring that highly skilled professionals spend hundreds or thousands of man hours poring over log data.

Oracle Audit Vault consolidates audit data generated by Oracle and non-Oracle databases from across the enterprise into a central repository and provides dozens of audit and compliance related assessment reports covering privileged users, account management, roles and privileges, object management and system management. *Oracle Audit Vault* provides built-in alerting for suspicious activity as well as attestation for reports and email notification, requiring that designated individuals review reports. *Oracle Audit Vault* also provides integration with ticketing systems such as BMC Remedy. Oracle databases audit settings can be centrally managed using the *Oracle Audit Vault* console.

How Oracle Controls Access to Patient Information

Implement Centralized Access Control

Health care is a dynamic, complex environment, with thousands of physicians, nurses, lab technicians, researchers, therapists, and support personnel, from front desk receptionists to IT professionals. All are linked electronically through LANS, WANS, and a wide range of wireless systems and devices. They are no longer simply concentrated in hospitals but across a distributed complex of primary care facilities, rehab centers and medical practices. Some may work remotely and access patient information as they travel.

HIPAA requires that health care providers implement policies and procedures for authorized access to PHI and technical policies and procedures for electronic information systems that maintain PHI.

Effective access management requires centralized authentication, authorization, and auditing, so that access control can be maintained efficiently, according to policy, in this type of environment.

To protect patient information and comply with HIPAA Privacy and Security rules, Health care organizations should define global policies for access to PHI and other relevant client data based on criteria such as:

- Need-to-know and context. Is this essential to perform the individual's job duties? A receptionist or database administrator has no need to see PHI. A lab technician may need medical information to perform his or her task, but doesn't need all of a patient's medical information.
- Privilege/authorization. Does the individual need to be able to copy and/or modify PHI, or simply read it?
- What applications have access to PHI?
- Who requires access to those applications? In what context (when and under what conditions the user may access the application) and what functions/capabilities of the application the user is authorized to use?

Effective access management—ultimately controlling who has access to PHI and how they are allowed to handle that information—should be centralized to work in large, distributed environments such as modern health care organizations. Without it, authorization and authentication for each application and resource is fragmented, likely to produce security gaps and burdensome to IT personnel and end users. Furthermore, determining, implementing and enforcing appropriate authentication levels for access to PHI and other sensitive information can become highly problematic under these conditions.

Producing auditable reports for internal use, partner requirements and HHS and/or state investigators is difficult, as administrators have to collect and query logs across diverse applications and systems. That means time, money and mistakes.

Oracle Access Manager secures access control through centralized authorization, authentication and audit, enabling single sign-on capabilities transparent to the user. It scales natively to bring centralized management to Oracle ERP, CRM and collaboration suite applications and provides out of the box integration and APIs to commercial and custom applications.

By separating authorization from the application, health care providers can efficiently manage and monitor access privileges across the organization and supporting facilities and personnel. Using *Oracle Access Manager*, health care organizations can assign authentication based on the application, system and/information that needs to be accessed, including user ID and password, X.509 certificates, smart cards, two-factor tokens and forms-based authentication. They can establish hierarchies of authentication, so that users might need simple ID and password for an employee portal, but two-factor token authentication for an HR self-service application.

Oracle Access Manager provides comprehensive security, operational, and compliance reporting, as a wide range of information can be logged into Oracle or any relational database and exported to third-party reporting engines or further analyzed through *Oracle Identity Analytics*. Common audit reports include: authentication statistics (success/failed rates across all access servers), authorization statistics (success/failed rates across all access servers), failed authorizations (by user), failed authorizations (by resource), access testing, group history (all changes to all group profiles), identity history (by user), locked-out users, password changes, users created/deactivated/reactivated/deleted, user profile modification history (for all users), deactivated users report and workflow execution time.

Access to protected resources can be controlled by user, group, role and attributes.

Use Role-based Access Control

Using a role-based approach provides a highly granular and flexible method for assigning and controlling access. Rather than relying on assigning privileges to individuals and/or individuals, to groups, a coarser approach that can become unwieldy and difficult to manage, roles can be assigned to individuals, making it easy to add or change responsibilities.

Oracle Identity Analytics provides policy-based role creation and automated role provisioning based on the health care organization's information resources -- such as employee white pages, reporting structures and partner and customer information -- which can be consolidated and leveraged in a centralized repository.

Oracle Identity Analytics is tightly integrated out of the box with *Oracle Identity Manager* to automate accurate user provisioning based on changes in role assignments (new hires, job changes, project assignments, etc.) or changes in business role and IT role mappings.

Automate User Provisioning

Even the best role-based access control policies and procedures can be derailed by poor user provisioning. Sound security and compliance practice requires a policy-driven management process for provisioning and de-provisioning user access privileges, a clearly established and thoroughly documented request, and approval and verification workflow.

The problem is that user provisioning is often both inefficient and inaccurate, as the brunt of the work falls on overtaxed IT administrators and help desks. Users and managers may navigate around required procedures and administrators may take shortcuts around policy. There will be serious gaps between policy and practice. As a result, users will wind up with inappropriate access to PHI, rogue or "ghost" accounts will remain active long after the individual has been terminated or changed roles, and health care providers will be in a tough spot at audit time.

Oracle Identity Manager provides centrally managed and automated provisioning of user access and authorization, assuring that users will have access to PHI based on job function and context, so that authorization can be provisioned and de-provisioned on demand, according to need, Health care providers can employ both role- and attribute-based automated provisioning, best realized through its tight integration with *Oracle Identity Analytics*.

Oracle Identity Manager supports separation of approval and provisioning workflow and provides a workflow "visualizer" that offers a graphical representation of workflow processes.

Oracle Identity Manager addresses the problem of connecting disparate systems, providing preconfigured connectors for the most popular commercial applications and interface technologies out of the box, enabling quick and scalable deployment in modern large, complex distributed health care organizations. In addition, Oracle's Adapter Factory technology provides rapid integration to commercial or custom systems.

The reconciliation engine detects any unauthorized accounts or changes to user access privileges and takes corrective action, such as undoing the change or notifying an administrator. Reconciliation, in conjunction with access denial features and workflow controls, allows organizations to detect and eliminate rogue and orphaned accounts.

Oracle Identity Manager provides historical and current provisioning data for compliance reporting, including user identity profile history, user group membership history, user resource access and entitlement history. This can be combined with the transaction data from workflow, policy, and reconciliation engines to address audit inquiries.

Deploy Secure Federation

Health care providers increasingly depend on an extended network of business associates, service providers, third-party support, vendors, etc. who need some level of access to internal applications, systems and information, including, in some cases, PHI.

If managing access control and authorization inside the organization is problematic, managing access for outside parties is far tougher. Typically, organizations have had to implement "one-off" procedures and processes with each party, requiring shared identity and authentication information, policy agreement and complex mutual authentication. Identity integration is costly and difficult to repeat. This is on top of all the usual headaches associated with access control and user provisioning.

Oracle Identity Federation is a scalable, standards-based and secure solution, which enables health care organizations to rapidly establish secure, repeatable and sustainable partner relationships, minimizing the recurring costs, integration issues and security risks generally associated with federation.

It supports multiple federation protocols, including SAML, Liberty Alliance and WS-Federation, support for Microsoft CardSpace for authentication as well as a wide range of authentication providers. Its flexible and scalable architecture can be integrated easily into heterogeneous environments.

Reduce Risk and Fraud

Patient information is increasingly exposed to high risk in this highly distributed and extended health care environment. As the transmission of digital PHI and associated patient information becomes prevalent, the risk of theft and fraud grows as Web applications reach out over the extended health care organization and across the public Internet.

Oracle Adaptive Access Manager helps secure this growing environment, making it safer for health care organizations to expose sensitive data to remote employees, health care providers, partners and patients. It provides real-time and context-aware risk assessment, multi-factor authentication and authentication process hardening for Web applications. *Oracle Adaptive Access Manager* reduces fraud and secures the free flow of information necessary for responsive health care.

Oracle Adaptive Access Manager provides two integrated components to help organizations prevent fraud. Adaptive Strong Authenticator provides methods to strengthen standard authentication mechanisms, innovative secondary authentication mechanisms and easy integration of third-party authentication products. Adaptive Risk Manager provides flexible context-aware risk analytics to protect applications across multiple channels of access. Real-time evaluation of multiple key data types can stop fraud when it is being attempted.

Conclusion

HITECH presents health care providers with both opportunities and challenges. The move to pervasive use of electronic health records, spurred by billions of dollars in incentives, promises a far more efficient, more responsive and, ultimately, more cost-effective health care system, tied together in a health information network that promises enhanced medical care.

This progress comes with a renewed emphasis on patient information privacy and security, put at greater risk by the very innovations in the use of electronic records that hold so much promise. Given the risk and rewards, as well as the clear message that they can expect elevated oversight from HHS and state governments, health care organizations must implement security programs built on sound data security, access control and authorization policies and standards-based controls.

Oracle's integrated and robust identity management and data security solutions, empower organizations to implement first-class security and HIPAA/HITECH compliance programs in health care's emerging electronic age.

Legal Disclaimer

The contents of this white paper are provided for general information purposes only, on an "AS IS" basis without warranty of any kind. The contents are not intended, and under no circumstances may be used or relied upon, as legal advice. If you have any questions about your organization's legal or regulatory requirements, please consult with an attorney.

ORACLE®

HITECH's Challenge to the
Health Care Industry
October 2011
Author: Oracle

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

Oracle is committed to developing practices and products that help protect the environment