

# Demystifying HIPAA Compliance: Security & Business Continuity

*An Oracle White Paper*  
*May 2002*

# Demystifying HIPAA Compliance: Security & Business Continuity

## EXECUTIVE OVERVIEW

The purpose of this document is to facilitate an understanding of the broad range of available solutions that can help address the security and business continuity targets of the Healthcare Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191), also known as the Kennedy-Kassenbaum Bill.

## INTRODUCTION

Industry pundits have long promoted HIPAA as the catalyst for e-business in the healthcare industry. While HIPAA imposes new administrative burdens on healthcare providers, payers, and clearinghouses, the law is designed to simplify the transfer of health information between organizations, increase efficiency and decrease costs associated with the healthcare system, and provide guidelines from the privacy of patient information.

However, due to the complexity of HIPAA, many are confused as to what actions to take towards complying with the guidance set forth in the legislation.

To begin, HIPAA affects most organizations that either provide healthcare or support and/or transact business with other health-related organizations. As a result, HIPAA affects employers, financial institutions, information technology outsourcing vendors, and ISPs. Thus, it is important for all employers, financial institutions and vendors that interact with the healthcare industry to first understand their liabilities and secondly, implement the appropriate solutions.

Of the five major parts comprising HIPAA, the Administrative Simplification Act most affects Information Technology systems. The Administrative Simplification Act calls for industry standard electronic data interchange (EDI) combined with stronger security standards that will ultimately guard against fraud, abuse, and eliminate unauthorized use of healthcare information.

Approximately five billion medical claims are filed annually in the U.S. with less than 20% of those submitted electronically. There exist over 400 different standards through which transactions can be electronically delivered. This ultimately leads to significant overhead in IT systems development and maintenance, and the next to impossible challenge of providing an environment that facilitates a sustainable level of information assurance.

**Many in the healthcare industry conclude that the security and privacy rules will have the biggest holistic impact on the operations of healthcare organizations (HCOs) and possibly the largest associated risks if compromised.**

**In essence, the Security Standard defines “how” healthcare organizations need to protect health-related information while the Privacy Standard specifies “what” individual health information must be protected.**

In addition to administrative simplification, HIPAA also mandates broad rules related to the privacy and security of health information. The HIPAA privacy rule mandates new policies on patient rights and the communication of medical information. The proposed HIPAA security rule suggests administrative, technical and physical best practices for protecting health related information.

HIPAA noncompliance may result in heavy fines, imprisonment and/or litigation. Penalties for intentional or negligent violation of the Act may include up to ten-years in prison and/or up to a \$250,000 fine. Perhaps more significant is the risk of civil litigation which may result in large monetary expenditures, loss of revenue, negative public relations, and the loss of customer/patient trust.

As of this writing, privacy regulations have been promulgated and security regulations exist in draft form. Guidelines for HIPAA certification or enforcement by the Office for Civil Rights (OCR) have yet to be determined. Unlike the transaction ruling, where the target for compliance is more tangible (ANSI X.12 for the transaction envelope, and various standardized code sets that define the envelope contents), the proposed security and privacy rules provide more generalized guidance to the end goal of compliance.

Ultimately, the onus is on healthcare organizations (HCOs) to determine the threat level and risk of occurrence for compromised patient confidentiality and/or fraud along with the associated consequences. It is this determination that forms the basis for security and privacy targets that will be met through the formulation of formal policies, procedures, and the implementation of technology via the remediation process.

## **WHAT IS THE IMPACT ON HCOs?**

HCOs must assess their existing policy and technical infrastructure to determine the level of risk exposure and map to new HIPAA requirements by:

- Developing appropriate policies and procedures to ensure that personally identifiable and sensitive data is appropriately collected, used, protected and, where appropriate, shared
- Providing safeguards through technical and physical tools that facilitate the implementation of the policies and procedures
- Deploying systems that implement the above in an effective and efficient manner with a high level of security assurance

The results of this mapping should provide a useful blueprint to what practice, policy and system upgrade changes may be needed to comply with HIPAA. Because compliance for the HIPAA security and privacy rules is much more open to interpretation and ultimately left up to the HCO to determine, it is critical that HCOs be able to prove due diligence in their evaluation and implementation of processes, policies and systems. This concept flows to the technology selection process. For example, the selection of products that have independent, third party

validation and verification (i.e., the products have been “evaluated”) provides neutral comparative criteria in helping with the product selection process. Additionally, this supports due diligence by providing the HCO with third party reviews of product function and security.

Evaluations are generally done against known standards. There are multiple national and international security standards to which a product can be evaluated. The standards process not only reviews the product, but also the product development process to ensure that security is an integral part of development. The most commonly accepted security standard is ISO 15408, or the Common Criteria.

It should be noted that much of the HIPAA guidance for security and business continuity has origins from guidance published by the National Institute of Standards and Technology (NIST, formed as a result of the Computer Security Act of 1987) for the handling of “sensitive but unclassified data”. Many government and other secure organizations have abided by these best practices for information assurance for the past 15 years. Although these standards were not originally designed for the healthcare industry, their relevance is nonetheless still significant to establishing a sound security implementation.

**“66% of health care providers said their top priority would be upgrading security on IT systems to meet HIPAA requirements”**

**- Healthcare Information and Management Systems Society (HIMSS) Survey**

As the security implications of HIPAA may be the biggest challenge to compliance, the best objective from a high-level is to reduce the impact of threats and the likelihood of their occurrence. To accomplish this, organizations must undertake a few steps:

1. Establish a baseline of existing policies, procedures, and IT infrastructure.
2. Determine operational practices that meet compliance requirements.
3. Perform an analysis to identify the gaps that exist between compliance requirements and the current baseline.
4. Identify the tools or raw materials to construct a secure environment.
5. Develop a process, or blueprint, that uses the tools to construct a system of policies, procedures, and technology that eliminates the gaps identified in step 3.

Organizations perform assessments to determine the level of remediation required to prevent against the disclosure, alteration, and destruction of information. The process of 1) analyzing an organization’s possible threat and vulnerability scenarios and 2) producing a tangible value of potential loss is called a risk analysis. Many HCOs have recently completed, or are currently performing, a HIPAA risk analysis (also referred to as an HIPAA impact analysis or gap analysis).

In a simplified view of risk analysis, the first step is to determine the assets being protected and their associated value. These assets may include, but are not limited to, patient information and the information communicated between business and healthcare community partners on a daily basis. Next, threats to the assets have to be considered. And lastly, a rate of occurrence (or the overall likelihood that the

threats will happen) is determined. When taken together, this information can be used in cost-benefit equations to ascertain how much it will cost to protect assets from varying threats.

Often, there is a direct relationship between the amount of money spent to secure an asset and the level of security provided. Normally, it is not practical to spend more on protecting an asset than the cost of replacement. However, while patient information may be replaced at a low cost, patient trust and HCO reputation may not. A proper risk analysis will hopefully illuminate these points and drive a prudent technology buying decision.

## **CHOOSING THE APPROPRIATE TOOLS**

Oracle has been at the forefront of developing robust security technologies for the past 25 years. As a result of this commitment, the Oracle 9i product suite delivers a robust, independently validated and verified technology to anchor a HIPAA solution by providing the information architecture needed to help protect the integrity, confidentiality, and availability of healthcare data. The Oracle 9i product suite helps organizations address security challenges through:

- Deep data protection - ensuring well-formed, comprehensive security from client to application server to data server, as well as throughout the layers of an application
- Internet-scale security - allowing user and privilege management to scale to hundreds of thousands of users accessing data
- Secure hosting and data exchange - enabling economical, secure partitioning of data access by customer or by user, while supporting secure data sharing among communities of interest

The following five items are used as the tools to provide information assurance:

### **1. Identification & Authentication**

This is the process of correctly identifying the users and authenticating them to the system. For instance, the identification process may consist of a username, and the authentication of the user consists of a valid password.

Within Oracle, there are ways to authenticate based on not only something you know such as your password, but also something you have such as a smart card or a X.509 certificate, or even something you are (biometrics) such as a finger print. Combining something you know with something you have (two-factor authentication) in a token card will provide an even higher level of assurance during the authentication process.

### **2. Authorized Privileges & Access Control**

Once the user is known to the system, their authorizations or privileges can be obtained. This is usually done in conjunction with an access control policy that defines what the user can and cannot do based on the privileges associated with

**The Oracle database provides robust technology to anchor a HIPAA solution by including such features as: state of the art security labeling, fine grained access control, auditing, encryption, and high availability options.**

the user and role. For administration purposes, Oracle will even let you define these in a single sign-on environment, such as a lightweight directory access protocol (LDAP) compliant server, so there is a single place to administer the enterprise security privileges regardless of the databases or applications.

It is important to also consider how these privileges can be turned on and off based on a user's roles or access profiles. Secure application roles within Oracle ensure privileges are highly restricted and cannot be turned on inadvertently or incorrectly. As an example, the privilege to read a patient record could only be enabled when accessing the database through a specific application, during specific times (or job shifts), and when the user had authenticated by a specific process.

Furthermore, access control may need to extend beyond the basic data structures to go within the data itself. For example, patient data should only be viewed by people that have a "need to know" about that particular patient's medical information. Other patient records within the same database should not be accessible. It is important that security be tightly coupled with the data to ensure that security cannot be bypassed and is consistent regardless of the application trying to access it.

**Traditionally, developers have built clever security schemes in applications. While this approach protects information from unauthorized access while persons are accessing data through the application, the security model does not apply once the data is accessed outside of the application.**

Traditionally, developers have built clever security schemes in applications. While this approach protects information from unauthorized access when accessing data through an application, the security model does not apply once the data is accessed outside of the application. For example, access to sensitive information through the use of a reporting or ad-hoc query tool would not guarantee the same level of protection because the security model only applies while a healthcare worker is using the application. For each additional application built, the security must be recoded and maintained in multiple places. In many cases, this problem is compounded as employee turnover leaves orphaned code that no one else on staff understands. Implementing security at the lowest level provides a higher level of assurance that confidentiality is maintained, no matter the method of access, and reduces development and maintenance costs.

### 3. Confidentiality

Patient privacy is synonymous with confidentiality. Access controls have to ensure that there is no accidental or unauthorized disclosure of data. A standard process for ensuring high confidentiality is encryption. Encryption has to take place as data flows in and out of the database and from a client to a middle-tier application or web server. Network intrusions are the easiest and highest occurring external threat, so encrypting network traffic is not optional, it is essential.

Oracle provides the technology to encrypt information from an Internet client using Secure Socket Layer (SSL) and from a middle tier server to a database using DES, triple DES, or RC4 algorithms.

Another form of encryption, selective database encryption, will allow data within the database itself to remain encrypted. In this manner, confidentiality in the database can be preserved. Sensitive data can remain encrypted and hidden even from administrators who have to perform routine maintenance tasks on the database itself. Their job usually mandates full access to all information. Encrypting sensitive data maintains the confidentiality in spite of this. Oracle's Advanced Security Option and database encryption toolkit provides a simple, off-the-shelf and unobtrusive way to provide confidentiality.

#### 4. Integrity

Measures should be in place to ensure that data does not get unintentionally or maliciously altered. Maintaining the integrity of the data should be one of the highest priorities. Data integrity can be provided through a data checksum, i.e. a technological verification that the data is as it was when originally sent or saved. This integrity can be implemented for data in motion on a network and at rest in the Oracle Database by using proven algorithms MD5 or SHA-1. Integrity can also be provided through fine levels of access controls and the ability to maintain a least-privilege environment. Least-privilege means that a user has only enough privileges to do their job and nothing more.

Oracle provides multiple methods for controlling access to data: user-based access, role-based access, context-based access, and label-based access. In Oracle, there are a high number of privileges that can be granted to users or groups of users, called roles. This high-fidelity in granting privileges facilitates the least-privilege concept. An example of roles that could be used in an HCO, include: a doctor, a nurse, a volunteer, or an administrative personnel.

One important and often overlooked aspect of access control is that it pertains not only to objects but also within the objects themselves. While user and role access determines who can access a specific object, it is the context-based and label-based access that determines which records within an object are actually accessible.

Regardless of whether managing object access or record access, the security mechanism needs to be tightly coupled with the data it protects. For example, in many situations creating database views with functions to implement context-based security is not the best approach, as there can be both security concerns and performance problems using this method.

Oracle's Virtual Private Database is an excellent example of a mechanism providing context-based security that is locked to the data it protects. In this mode, the server automatically enforces the access control within the object(s) it protects thereby giving a higher level of assurance that data integrity (and confidentiality) will be preserved.

Oracle Label Security (OLS) provides label-based access control. OLS can ensure that unauthorized users cannot view or alter the data. OLS labels data

**The United States Military Health System (MHS) chose Oracle and its security infrastructure to enhance its ability to manage, access and deliver critical patient/provider data when needed. The MHS also has built its integrated, enterprise-wide Electronic Patient Record system on Oracle.**

and only users with the appropriate clearances (or user labels) can see and/or modify the sensitive records. The concept of labeling data has historical ties to government systems that require multiple levels of access (e.g., secret, top secret). This is often referred to as multi-level security, where both the data and the person accessing the data have assigned security labels.

A possible scenario in healthcare would be a labeling scheme that assigned values to data based on the following sensitivity: Public, Internal, Confidential, and Restricted Confidential. The determination of appropriate label would be based on the risk assessment if the data were to be compromised. For example, a patient's diagnosis code might be considered "Restricted Confidential".

The combined use of roles, contexts, and labels offers multiple layers of security to protect the data – should one layer of security become disabled (or implemented incorrectly), the other layers would still be there to enforce security thus limiting potential exposure and the security risks.

## 5. Accountability

Accountability is the ability to track actions or behavior of users. This is provided through auditing. Auditing should not only include information indicating that a user accessed data; it should also track how he or she accessed the data – i.e., what was the exact query against the data. The reason this is needed is that it can be used to show the user's intent. Coupled with the audit logs and the ability to answer what it was that the user asked for is the ability to answer what the user saw. For instance, the user asked for John Doe's diagnosis. Did the user get to see the diagnosis, or were the results not back from the lab? This knowledge is invaluable to providing true accountability.

Oracle provides accountability in several ways. First, Oracle provides over 200 auditable events. Next, a feature called fine-grained auditing can be used to show intent by answering the question "what specifically did the user ask for?" Finally, Oracle's flashback query can use information contained in the audit log to answer the question "what data did the user view at that point in time?" For accountability purposes, this combination of technologies shows the user's intent and whether or not patient confidentiality was breached.

Historically, the challenge with auditing is the tremendous amount of data that are generated. Minimizing the logging of audits for access to a system or data based on normal operations (except in the case of an emergency) is paramount because these events are based on legitimate actions. For example, global auditing for all events might only be enabled during a "panic button" system override for a life or death situation. During normal operations, only specific conditions of data access would trigger an audit event. The ability to specify the exact event that triggers an audit not only helps to minimize system overhead, but also reduces the effort to navigate through audit logs to isolate a specific event.

Many instances of unauthorized access to information stem from rogue users who normally access sensitive information to perform their job on a daily basis. These users might be authorized to view sensitive data, but only in the context of job performance. An important feature of auditing is that it is extensible to track a “suspicious” query. Oracle fine grain auditing can be configured to track not only access by a particular user, but by virtually any type of question that can be asked of information.

Due diligence demands the employment of as many reasonable complimentary measures as possible. This layered security model, also known as security in-depth, is used by many industries that wish to protect their most valuable resources. It is also important that the measures employed be both intimately integrated into the information architecture and add as little processing overhead as possible. This unobtrusive approach allows for ease of integration without sacrificing system performance.

### **AN EXAMPLE OF INFORMATION ASSURANCE**

Oracle technology is an integral part of many existing healthcare systems that house sensitive data. The University of California San Diego School of Medicine developed the Patient Centered Access to Secure Systems Online (PCASSO), which contains over 178,000 medical records and provides trusted access to a patient’s own health information and access to a healthcare provider’s patient’s complete medicals over the Internet. Of particular note is that this system represents the most sensitive data traveling over the most insecure medium.

The application stores sensitive patient history that includes information related to HIV/AIDS, abortion, mental health, sexually transmitted diseases, and genetic information. The context-based control that Oracle Label Security provides was an ideal solution for providing the correct access to information with a high level of assurance. The assurance is derived from the following facts:

- The technology is evaluated
- The implementation of the security mechanism requires no application coding
- The security is locked to the data it protects and therefore cannot be subverted

### **USING PROVEN SECURITY SOLUTIONS**

For HIPPA compliance, the critical decision comes down to deciding between the cost of implementing effective security and the cost of doing nothing. The best way to reduce overall costs is to obtain security from proven off-the-shelf software vendors who implement their solutions based on standards. A perfect example is Oracle’s network encryption capabilities that come with the Oracle Advanced Security Option (ASO). This technology has been independently evaluated and proven to be implemented correctly. Because of this formal evaluation, ASO can

**Only the Oracle 9i database has been certified by 14 independent security evaluations, far ahead of any other technology provider.**

be configured in a mode compliant with the U.S. Federal Information Processing Standard (FIPS) 140-1 Level 2. Level 2 is the highest possible level that can be attained by a software product. The security algorithms are known and proven standards (e.g., DES, RC4, SHA-1, and MD5). Furthermore, enabling this feature is completely unobtrusive to existing and future applications – the applications don't have to be modified to take advantage of the additional security. In this scenario the cost of the security feature is compared with the cost of violated patient confidentiality when an internal or external intruder eavesdrops the network.

## **PROVIDING CONTINUITY TO BUSINESS OPERATIONS**

The HIPAA legislation also stresses that formal disaster recovery and business continuity policies and procedures be formally developed. Many HCOs have extreme requirements for high availability of data, especially in times of critical or emergency operations. These organizations also require rapid recovery from system failure and continuous operations while normal system maintenance is performed.

Within Oracle's technology there are numerous high availability features. Examples of these include the ability to quickly recover from data corruption and the ability to perform routine maintenance or adjust configuration parameters while a system is available for production use.

The highest levels of availability must ensure against single points of failure. Hardware vendors can assist with connected computers (or clusters) that house database files on shared disks. If a computer (or node) in the cluster should fail, the disks can be activated on another node and processing can take place on a surviving node. However, the outage time required for such a failover can be more than a customer could tolerate. Any database instance itself is a single point of failure.

To this end, Oracle provides multiple instance database protection with Real Application Clusters (RAC). In a cluster, each node runs an instance of the database. Critically, each node has access to all the data in the database. Should one node fail, fail-over time is virtually eliminated and users avoid the downtime associated with reestablishing their connection to the database. With RAC, applications within a datacenter enjoy a high level of fault tolerance with increased performance through the scalability of additional clustered servers.

In many scenarios, one additional step is taken to ensure fault tolerance for a geographical outage. Oracle Data Guard can be configured to mirror information to identical configurations in offsite datacenters. Should the production datacenter become unavailable, the production environment would switch to the secondary site instantaneously.

**High availability means that your applications are available 24/7 and that failure of hardware should not affect your operations or data. Oracle9i Real Application Clusters meets these requirements since each server acts as a fail-over machine for all other servers in less than 60 seconds.**

## **CONCLUSION**

It is the responsibility of HCOs to determine the value of their information assets, determine the threat risk to those assets, and the annual rate of those threats occurring. From these determinations, a formal security model, made of up policies, procedures, technology, physical measures, and awareness can be put into place.

The pillars of security are built on good technology, best practices and methodology, coupled with a high degree of assurance that technologies and processes are implemented correctly. There are many aspects to accomplishing these goals, technology being just one part. As the amount of sensitive information stored electronically increases, combined with increased access through multiple channels – the inherent vulnerability risk associated increases as well. There has to be support for proper identification and authentication, authorizations and access controls, confidentiality, integrity and accountability. These tools need to be combined with good process and proof that an organization has done its best to ensure a successful HIPAA strategy.



Demystifying HIPAA Compliance: Security & Business Continuity  
April 2002

Authors: Michael Donlan, David Knox

Contributing Authors: Joe Alhadeff, Justin Pearlman, Marshall Presser

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  
[www.oracle.com](http://www.oracle.com)

Oracle is a registered trademark of Oracle Corporation. Various product and service names referenced herein may be trademarks of Oracle Corporation. All other product and service names mentioned may be trademarks of their respective owners.

Copyright © 2002 Oracle Corporation  
All rights reserved.