Successfully Negotiating the HIPAA Maze

A Sybase, Inc. Healthcare Report on Complying with Administrative Simplification & Security Mandates

WHITE PAPER

New Era of Networks®

A Sybase Company

SYBASE®

NFORMATION ANYWHERE™

Table of Contents

Executive Summary - Key Points:

- Touted as the most complete solution available today, HIPAA Accelerator (formerly Paperfree®) gives healthcare organizations the technology needed to develop and implement HIPAA administrative transactions.
- HIPAA Accelerator is powerful enough to be used by the largest healthcare organizations. It is easy to use, quick to install, and simplifies the process of meeting government-mandated deadlines for HIPAA compliancy.
- Sybase delivers a customizable HIPAA solution with our Sybase Enterprise Portal, that provides comprehensive security to maintain mandated privacy regulations. This also creates a self-service environment in which providers and consumers can get personalized, authenticated access to the information they need, whenever and wherever they need it, saving you lots of administrative costs.

Overview

Sybase has created this white paper to explore the challenges healthcare organizations are facing with the Healthcare Information Portability and Accountability Act (HIPAA) and the steps needed to successfully negotiate the many aspects of the regulations. It also serves to demonstrate Sybase's dedication to providing customers with answers concerning the changes in security and transaction standards and how Sybase products enable the move toward compliance.

HIPAA Summary

While HIPAA is seen in the eyes of some as one of the most monumental tasks the industry has ever faced—even outstripping that of year 2000 preparations—it is the intentions of Congress and Health and Human Services that administrative simplification will save the industry billions of dollars. This will occur when HIPAA simplifies the complex process of administration and payment of healthcare claims by implementing a single transaction standard in place of the nearly 400 currently being used by the industry. Not only will HIPAA define a single transaction standard, but also code sets used in the transactions. The regulations also require a national standard for identifying the different entities within the industry and establish security and privacy standards to protect the increased usage and transfer of electronic data. Naturally, while the initial phases of compliance will be a large step for all involved, HIPAA will eventually cause a substantial improvement in efficiency and reduce the costs associated with delivering care to patients.

HIPAA regulations apply to all payers, clearinghouses and providers who choose to utilize electronic methods for transactions. Specifically, under the enacted regulations, health plans will be able to reimburse providers, authorize services, certify referrals and coordinate benefits utilizing a standardized electronic format for each transaction. Additionally, providers will be able to check eligibility for coverage, check claim status, request referrals and service authorizations, as well as receive electronic remittance to post receivables. Other transactions fall under the standards as well, and include coding standards for reporting diagnosis and procedures in the transactions. Also included under the provisions is a way for employers who provide health insurance to use a standard electronic form to enroll or purge employees from their plans and to submit premium payments to the health plans they choose to engage.

Making the Move: The First HIPAA Deadline Approaches

While privacy and security frequently have been the focus of much that has been said and written about HIPAA, it's the transaction standards that the industry will have to confront first. The final rule for transaction standards has been issued and, barring any attempts by Congress to alter them, will be enforced beginning October 16, 2002. Six months later, on April 14, 2003, the rules on protecting patient data will start being enforced.

What this means is that in a little more than a year many healthcare organizations who will be completing transactions electronically will have to comply with the new standards as mandated by HIPAA. There are a few exceptions. These include:

- Small health plans: These are health plans with less than $5 million in transactions annually. They have an additional 12 months to comply.

- Health plan sponsors: These consist of any health plan that serves as a sponsor or employers who self-insure. Exempt from the HIPAA mandates are property/casualty and workers' compensation insurers, and self-administered employee health benefit plans with fewer than 50 participants.

- Workers compensation: Plans such as this are excluded from HIPAA regulations, are property and casualty insurance plans because, while they may cover some health benefits, are not considered health plans under the strict definition outlined by HIPAA.

Standards and Codes

Unlike Y2K, HIPAA won't be a one-time problem that can be addressed at the last second. HIPAA is ongoing and the regulations are subject to change. That's because HHS will continue accepting and evaluating requests for changes to the standards and then recommend those changes to the Secretary of HHS. The six organizations designated to serve as the Designated Standards Maintenance Organizations (DSMO) are:

1. Accredited Standards Committee X12
2. The Dental Content Committee
3. Health Level Seven
4. National Council for Prescription Drug Programs
5. National Uniform Billing Committee
6. National Uniform Claim Committee

The Secretary of HHS may modify a standard or its implementation guide specification one year after the standard or implementation specification has been adopted, but not more frequently than once every 12 months. If the Secretary modifies a standard or implementation specification, the implementation date of the modified standard or implementation specification may be no earlier than 180 days following the adoption of the modification. HHS will determine the actual date, taking into account the time needed to comply given the nature and extent of the modification. HHS may extend the time for compliance for small health plans. Standards modifications will be published as regulations in the Federal Register.

However much change occurs to HIPAA regulations, the initial standard for transactions has been decided. That standard—ANSI ASC X12N, Version 4010—will be the driving force behind the consolidation between the disparate methods currently being used. It is to be used for all healthcare transactions with the exception of those from retail pharmacies. They will continue to use the standard maintained by the National Council for Prescription Drug Programs (NCPDP) because it is already widely used. The NCPDP Telecommunications Standard Format Version 5.1 and equivalent NCPDP Batch Standard Version 1.0 are the adopted formats, and health plans will have to support one of these formats, in addition to ASC X12, to meet HIPAA requirements. According to the regulations, transactions subject to the ASC X12 standard include:

- Enrollments and benefits maintenance (834)
- Health plan eligibility (270/271)
- Claim payment and remittance advice (835)
- Premium payments (820)
- Claim status (276/277)
- Claim submission for professional, institutional and dental (837)
- Health care services review (278)

It is widely believed that there might be a need to complete mass upgrades to technology infrastructure in order to comply, but this isn't necessarily the case. For instance, companies can utilize devices that convert legacy data into the standard format for transmission and convert it back to the base format so it can be utilized internally. In other words, HIPAA transaction standards apply directly to data that are being sent and received electronically, with the exception of data sent inside corporate entities and between federal agencies and their contractors or between state agencies. This means that while stored it can exist in any format. However, that data must always remain secure from inside and outside disclosure (more on this later). And if it is transferred by CD or magnetic media data must comply with the standards, as well.

A big hurdle for organizations becomes determining which data must be transformed to meet the guidelines and which data doesn't. Health and Human Services recommends asking the following questions to determine what is required:

Question 1: Is the transaction initiated by a covered entity or its business associate? If not, the standard need not be used.

Question 2: Is the transaction one for which the Secretary had adopted a standard? If yes, the standard must be used. If no, the standard need not be used.

Besides moving the industry to a single transaction standard, HIPAA is also mandating standard code sets, which are designed, as are the transaction standards, to help improve the efficiency and ease with which the industry operates

Identifying Employers and Providers

HIPAA also seeks to implement a national identifying number for providers and employers, as well as health plans and individuals. The employer ID will probably use the employer's tax ID number. The creation of provider ID numbers and national plan ID numbers are still in the works. In addition, the creation of a national patient ID faces barriers to implementation and may never occur.

The idea behind standard identifiers is to improve Medicare and Medicaid as well as other health programs by reducing redundancies and the possibility for errors when identifying entities involved in the processes associated with normal health-related transactions. And while these provisions have yet to be set in stone, they will certainly have an impact on the industry and eventually may include individual identifiers that patients keep with them for life.

The Next Step: Addressing Privacy and Security

Just six months after the transaction standards are enacted, on April 14, 2003, the rules on protecting patient data will be enacted. These rules mandate that patient identifiable data be portable, private and secure whether it's being stored, transmitted electronically or being moved on magnetic media. And though rules differ based on the size of the organization, any company that engages in electronic transmission of health-related data will need to address these issues and put a plan in place to protect personal information. This necessitates the establishment of not only internal policies, procedures and practices, but also a secure environment where data is protected from all breaches in security, both internal and external.

One of the most important aspects of compliance is education. Every healthcare organization not only needs to create security policies and procedures regarding HIPAA, but also educate employees on how to adhere to them. To boost compliance levels, healthcare organizations need to consider implementing ongoing training programs to educate employees on the new standards in addition to the organization's policies and procedures. Since HIPAA is an ongoing issue, rather than one-time-only event such as year 2000 concerns, training programs need to be an ongoing effort, whether the training takes place via traditional in-services or by computer-based training.

Achieving enough security to maintain HIPAA—mandated privacy will be a challenge for most organizations, especially considering that there are several areas that must be addressed under the guidelines. Information systems security: This pertains to protection of computers and workstations that get used for viewing and transmitting patient-identifiable data and related information. These terminals must be protected from both internal and external security breeches. Maintaining security for information systems may require risk analysis, access lists, configuration management, personnel security, password management, auto log on and off, internal audits, virus checking and incident management. Translation also may be an issue for organizations dealing with large quantities of legacy data—and systems—that will continue to be the cornerstone of their IT efforts after security and privacy guidelines have been implemented.

- Physical security: This means that the premises and assets must be protected from potential security compromises or threats. Included in this is unauthorized access to workstations, network or storage facilities. Items that should be considered for an organization's physical security include door locks, secure workstations/databases, access codes, secure back-up and storage, sign-in logs, and protection for multiple points of entry.

- Audit trails: Designed to help identify activity as it relates to patient-identifiable data, audit trails are key for any organization who is required to review all information access.

- Digital signatures: Different than identifier numbers, digital signatures are designed to ensure that information being transmitted electronically is authentic and protected from observation while it passes through intranets, extranets and the Internet.

- Privacy: One big area of concern is the ability for patients to have the right to review, address and comment on their medical records. Patients also have the right to know who has viewed their medical records, and have the right to prohibit their medical information from being viewed by certain people in certain situations

Chain of Trusts

Because the healthcare industry relies so heavily on information that moves quickly and in many directions, every healthcare group that intends to send data electronically will have to contend with chain of trust agreements. This addresses what happens to patient information once it has been collected by an organization. It's been estimated that a person who enters a hospital complaining of chest pains will have the related medical data sent to 28 different entities. Under HIPAA, the initial hospital where the patient was first seen has the obligation to ensure that every destination for the data is compliant. Ultimately, this means that any organization that falls under HIPAA will have to identify all their destinations for patient-identifiable data and enter into chain of trust agreements with those companies, which basically states that the receiving organization will maintain appropriate security measures to comply fully with HIPAA.

The Results of Data Disclosure

There are still many unidentified parts of HIPAA. For instance, who will end up being in charge of enforcing the rules and guidelines? Although the Office for Civil Rights (OCR) has been named as the "watchdog" for HIPAA privacy, it is still unclear who will be the watchdog for transaction compliance. Whichever agency it ends up being, it will be well within the group's right to, at any time, complete an audit of the books and records of an organization—and any business partner—to determine their level of HIPAA compliance. This is why every organization planning to use electronic formats for the transmission of data will need to be prepared. They also will need to have a strong understanding of the rather significant legal ramifications of misappropriating patient-identifiable data.

If a breach does occur, the covered organization can be fined anywhere from $100 to $25,000 per violation. There could also be criminal charges enforced for violations that are committed knowingly. Further penalties can result when organizations or individuals attempt to conceal security violations from HIPAA officials.

For organizations or individuals who attempt to obtain or utilize any personal health information with the express purpose to cause damage to an individual or organization, or to use it commercially could be fined up to $250,000 and serve 10 years in jail. Naturally, litigation also can result when business partners as well as individual patients sue the responsible parties over breeches that occur by accident or on purpose.

HIPAA's Affects: Rolling with the Changes

Nearly every nook and cranny of healthcare will feel the impact of HIPAA. From the executive level to the support staff, the rules will create the need for significant change, especially within departments that deal with patient data or the systems used to manage that data. To meet the quickly approaching regulations organizations must put a plan into action—if they haven't already.

It's recommended that each organization designate a HIPAA official who can oversee the move to compliance with transaction standards and privacy issues. The first step is to review existing laws and regulations at the state level. They differ from state to state and must be understood and taken into account during the move toward compliance. The next step is to review applicable federal regulations pertaining to privacy and security. All business partner agreements need to be reviewed and data has to be tracked so it is known exactly where it's going once it leaves the organization.

With this information a plan can be drawn up to take the company down the final stretch to compliance. As part of that, it's important for key executives within the organization to familiarize themselves with all parts of HIPAA and monitor closely any changes that are mandated, especially those changes that will have an impact on the organization. Part of the overall approach would also be to evaluate different vendors and identify a core group of companies that can help your organization successfully reach and maintain HIPAA compliance. It's imperative that they have a thorough understanding of the technical—as well as legal implications—of the mandate.

HIPAA Solutions

HIPAA Studio: HIPAA Accelerator with Compliance Verification and EDI Server

With the HIPAA deadline on the horizon, the healthcare expertise and solutions offered by Sybase and the HIPAA Studio can help organizations prepare. The HIPAA Accelerator and the EDI Server provide healthcare organizations the tools needed to make their data transactions HIPAA compliant. The EDI Server is made up of two key components, the ECMap Development Workbench and the ECRTP Execution Engine.

HIPAA Accelerator

HIPAA Accelerator (formerly PaperFree), coupled with the EDI Server, together simplify the efforts needed for healthcare organizations to become HIPAA compliant. The HIPAA Accelerator is an enhancement to ECMap and the EC Gateway™, a message management server. Together, these solutions simplify the efforts needed for healthcare organizations to become HIPAA compliant.

The HIPAA Accelerator consists of three components — HIPAA compliant X12 standards, HIPAA compliance maps for each X12 transaction and a suite of compliant test data. Compliance maps contained within the Accelerator allow users to verify that their transactions conform to the implementation guides. These robust compliance maps are fully open and allow the user to add, delete or change compliance rules as the customer sees fit. Additional rules can further narrow down the compliance maps to allow for business logic and flow. This is typically done for validation of information such as member numbers, provider numbers and dates of birth versus dates of service.

Compliance maps are essential for all organizations that will be directly sending and/or receiving HIPAA X12 transactions. In fact, the Centers for Medicare and Medicaid Services (formerly called the Health Care Financing Administration, or HCFA) has required that all Medicare intermediaries should procure translators that will validate the syntax compliance for the X12N 837 transactions, such as alpha numeric, field length, valid qualifiers, mandatory loops and segments, as well as appropriate segments within a given loop. The compliance maps are open and end-users can make edits to the compliance maps as needed.

As a result, end-users can add, change and even delete compliance checking rules to accommodate the needs of their healthcare organization.

Benefits

- Availability of the HIPAA standards and compliance maps can reduce development time by as much as six months
- Only those segments, elements and code values that are needed for the HIPAA transaction are shown resulting in more accurate mapping
- Easy to navigate graphical user interface (GUI) front-end combined with drag and drop mapping allows “non-technical” employees to easily develop translation maps

Features

- HIPAA X12N Standards in version 4.0 of the HIPAA Accelerator are based on the approved, final June 2000 Implementation Guides
- Compliance maps for each of the HIPAA transactions
- Test data and cases for each of the transactions
- HIPAA transactions at present include the following: Eligibility (270/271), Claim Status (276/277), Service Review and Response (278), Premium Payment (820), Enrollment (834), Claim Payment (835), and Claim Submission for Professional, Institutional and Dental (837)
- Future versions and updates of the HIPAA Accelerator are available by purchasing a product maintenance contract.

EDI Server Consists of ECMap and ECRTP

ECMap Development Workbench

The ECMap suite is a solution enabling the seamless transformation of large volumes of data among customers, suppliers and partners. With the ECMap suite, healthcare organizations can rapidly develop e-Business communities, support multiple message formats and manage greater volumes of transactions.

ECMap provides a complete solution that enables healthcare organizations to systematically manage heterogeneous business data and transaction channels. With ECMap, healthcare organizations can move data transactions in X12, HL7, XML, HTML, proprietary and other formats, shifting between them as needed and even sending data in mixed formats. For example, claim attachments, which may contain HL7 data imbedded directly within an X12 transaction, cannot be accommodated by many organizations. Yet ECMap can easily handle the HL7 data inside the message of the X12 transaction itself. Other features include:

- Any-to-Any Mapping: Industry standard and proprietary formats are mapped directly to or from the database, without pre-processing.
- Web Application Development: With ECMap, healthcare organizations can build sophisticated Web-based, n-tiered applications with ease.
- Business Rule and Flow Logic: Rules and associated flow logic are easily created within ECMap’s graphical user interface, and shared between maps reducing development time significantly.

ECRTP Execution Engine

ECMap’s execution engine, ECRTP, supports batch, fast batch (near real-time), and real-time data format integration for HIPAA transactions. ECRTP processing speeds are the fastest on the market, and provide for seamless integration with any ODBC-compliant database. Features include:

- Data Transformation: ECRTP converts data to or from back-end data sources, permitting high-speed integration to business applications. ECRTP can collect data from the Web or a database and create HTML at high-speed.
- Portal Empowerment: ECRTP allows end-users to permit trading partners to access multiple business applications across the Internet for data viewing or data collecting.
- Performance and Scalability: Healthcare organizations can permit trading partners real-time access to multiple back-end business systems simultaneously, allowing more informed business decisions.

Sybase Enterprise Portal

Many healthcare organizations are exploring the Internet as a way to achieve new levels of connectivity between providers, patients, payers and partners, and even increase employee self-service capabilities within their organizations. However, managing the frequently disparate and extensive data stores contained within most healthcare organizations takes robust technology capable of turning impersonal data into useful and accessible information, and making that information comply with HIPAA requirements. For these reasons, many organizations are utilizing enterprise portals to extend their businesses to the Web. This technology segment is growing significantly, with Merrill Lynch forecasting that the overall enterprise portal market will grow to be a $14.8 billion industry by 2002.

Sybase, with extensive healthcare industry and portal experience, has developed Enterprise Portal™ (EP), a comprehensive and agile technology solution that can improve communications and organize vast types of data into usable information. By surrounding current systems and leveraging existing information by integrating it with mainframe applications, data and events, or best-of-breed third-party solutions (including wireless and handheld devices), Sybase EP makes it possible to move business processes to the Web without the need to reengineer and redesign existing business operations. This allows rapid and low cost connectivity to physicians, lab results, best practice data, health plan information including eligibility, benefits, claims, provider directories, appointment scheduling and more. All in a quick and secure environment that allows the integration of leading and future technologies.

Sybase's EP security framework provides the comprehensive set of security features required for today's healthcare portals and HIPAA compliance, including:

- All sensitive communications with the portal are protected by encryption for confidentiality and integrity
- Secure access via wireless and handheld devices
- Single sign-on is supported across the portal
- Sybase EP authentication can be linked to enterprise login authentication, eliminating the need for a separate portal login
- Data can be digitally signed for non-repudiation of business transactions
- A minimum authentication strength can be specified for a component to ensure that only strongly authenticated users can access particularly sensitive data

Sybase Professional Services

To make all the pieces come together and ensure HIPAA compliance, Sybase supports its customers from development through deployment with an experienced professional services organization. Sybase Professional Services has years of healthcare experience building technology infrastructures, integrating disparate systems and ensuring data security. Sybase Professional Services has applications that reduce administrative costs, streamline operations and improve communication between all constituents within the healthcare continuum. To extend your business to the Web, Sybase Professional Services can help organizations build their portals faster and with lower risk than when they build it themselves.

Contact Information

Carol Fronduto
Healthcare Business Development Manager
561 Virginia Road
Concord, MA 01742
Phone: (978)287-2657
Fax: (978)287-1516
www.sybase.com/healthcare