HIPAA Compliance: A Technology Perspective

Richard Krohn

In a replay of Y2K, healthcare organizations are collectively focusing their attention on HIPAA solutions as the implementation deadlines loom near. Much has been written about HIPAA as a process issue, and that, at best, technology solutions can address 20 to 25 percent of HIPAA compliance requirements. In fact, the HIPAA rules do not specifically mandate technology solutions, and allow individual organizations to devise their own HIPAA compliance strategies. But the fact remains that technology — either as a primary HIPAA solutions driver, or as a support mechanism — remains a key ingredient of any comprehensive HIPAA remediation plan.

The HIPAA guidelines, still fully to be revealed as of this writing, formally govern four broad areas: transaction and code sets, privacy, data security, and provider identifiers. Of the four HIPAA categories, one requires the creation of standards (code sets), one requires creation of digital labels (provider identifiers), and two provisions — electronic transaction standards (data security) and privacy — suggest specific technology solutions.

Both of these latter categories contain a bewildering array of compliance issues. For instance, although HIPAA is not prescriptive, in general the data security provisions require compliance in the following areas: identification, authorization, encryption, data protection, auditing, access control, digital signatures, and disaster recovery. Obviously, no single data security architecture or application can satisfy the compliance criteria in each of these areas, across the spectrum of healthcare organizations. Healthcare IT managers must determine what mix of systems architecture(s), applications, and infrastructure should be deployed to meet the HIPAA standards in the “current state,” and they must anticipate the torrent of processes and transactions that are being moved to online media in answer to the ever-present need to cut costs — and that will certainly be subject to HIPAA scrutiny.

Technology to the Rescue

Conceptually, data security strategies and tools proceed from one or more of the following: what a person possesses (a card or an electronic token, for instance); what a person knows (a password); or what a person is (a biometric identifier such as a fingerprint or retina scan). These separate security architectures may be deployed individually or simultaneously, depending on the insularity of a healthcare organization, its information flows, and the magnitude of data sharing both within and beyond the organization.

For instance, a small physician practice is more likely to have static user access requirements, data transfers, and transaction-based relationships than similar conditions found in a hospital setting. For this reason, the data security requirements of smaller, less information-intensive healthcare organizations are less complex than larger, vertically oriented enterprises. As a result, HIPAA compliance security architectures proceed from basic access controls to sophisticated authentication, encryption, and user rights technologies.

Access Control

In its simplest form, data security relies on some combination of logon and password access control. Typically, password-protected systems are deployed in virtual private networks (VPNs), intranets, client/server networks, and other insular computer systems. At this level, security architecture can include physical access devices such as smart cards and tokens, which act as “keys” to unlock desktop security systems. Additional layers of security may be added within this architecture by the addition of user-specific firewalls.

For smaller healthcare organizations with limited users, limited data-sharing requirements, and limited budgets, this security architecture can meet the HIPAA standards of data security within the organization. However, password-protected systems are notoriously easy to defeat as the user population expands, and healthcare organizations that choose to rely on this level of security to meet HIPAA requirements must also impose corresponding procedures governing sharing, storage, and misuse of passwords.

Authorization and Encryption

Larger healthcare organizations maintain complex, unique, proprietary computing systems whose users each have a singular profile of access and activity requirements. These organizations require a combination of security architectures not only to control access, but to safeguard communication and information exchanges within and beyond the entity. To satisfy these requirements within a system architecture that is flexible, rules-based, and interoperable, many organizations elect to deploy a tiered security strategy. Tier one consists of a logon and password combination, and, in more technically advanced organizations, this sign-on procedure is replicated across discrete computing systems within the organization through the deployment of Single Sign-On (SSO) technology. SSO allows each user to employ a single access code among a host of “stand-alone” applications. Tier two consists of encryption technologies, such as Public Key Infrastructure (PKI), and secure connectivity technologies, like
Secure Socket Layer (SSL), as well as more exotic user identifiers such as biometric technologies. The primary features of these technologies follow:

**Single Sign-On.** This is a simplified logon procedure, in which a single password entitles the user to access multiple applications including web-enabled, legacy, and proprietary systems. There are two main types of SSO: workstation-based solutions, which simplify logon procedures but add no additional measure of security; and server-based SSO, which does add an additional layer of security into the solution. In larger organizations, scaleability and interoperability are chronic problems with enterprise-wide SSO. Consequently, SSO technology in its current state of development is best suited to deployment in less complex, insular computing environments, such as a clinic or group practice.

**Public Key Infrastructure.** PKI is an asymmetric encryption architecture that validates a user’s identity (through a digital certificate), applies sophisticated encryption/decryption technologies, and creates digital signatures. PKI consists of four main components: a certificate authority (that issues digital certificates); a registration authority (that maintains records of users); a policy framework governing certificate issuance and cancellation; and PKI-enabled applications such as web browsers and e-mail servers. By employing a combination of public and private digital “keys,” PKI provides a high degree of security and data integrity. PKI employs 40-bit and 128-bit encryption keys (a bit describes the length of an algorithm — the larger the bit size, the more complex the encryption).

PKI meets the general HIPAA standards for authentication, confidentiality, integrity, and non-repudiation. Typically, PKI is suited to organizations like hospitals that routinely relay large volumes of sensitive data between systems and among larger populations of users. This is particularly true of data transfers through web-based applications or between separate entities.

**Secure Socket Layer.** A symmetric encryption for web-enabled data transfers, SSL offers an added dimension of security. Like PKI, SSL employs public/private keys, but it additionally creates secure “tunnels” between servers and to web browsers, and vice versa (by creating time-sensitive “sessions”). This makes SSL an ideal application for conducting secure online transactions (such as online prescription ordering) and hosting e-mail applications. Since SSL requires a unique set of “keys” for each relationship, it is best suited for recurrent, sensitive data transfers among known parties. Ordinarily, these types of relationships are to be found in large-scale healthcare organizations such as health systems and networks.

**Biometric Identification.** This is a means of measuring individual human characteristics through techniques such as voice recognition, fingerprint identification, retinal and iris recognition, and other techniques. Since these characteristics are utterly unique, biometrics provides non-refutable authentication and user privileges. Biometrics work best in controlled environments, such as LANs, due to the sophisticated hardware and authentication systems required, which are unusable on a global basis.

**Digital Rights Management**

DRM refers to technologies that protect information throughout its life cycle by securing, monitoring, distributing, commercializing, and tracking access to any form of digital content. Unlike episodic encryption or authorization-type security technologies (like PKI and SSL), DRM continually governs a user’s rights to view, copy, print, store, modify, or forward digital content. DRM is still a new technology, and currently is being deployed intra-enterprise, but may soon be practical for public networks as well.

**Strategizing HIPAA Technology Solutions**

In the minds of many, HIPAA is the current version of Y2K, a costly exercise attended by a mild hysteria, and of dubious value. From the outset of a HIPAA technology initiative, it is vital to educate the leadership of the organization — from the board on down — about the urgency of HIPAA compliance, and to engage key managers as part of the project team. With any project whose impact will be felt throughout the organization, and whose constituents are wide-ranging, a data security initiative should proceed from a coherent project plan, implemented by a leadership team consisting of relevant stakeholders, and backed fully by senior management. This team might include professionals from areas such as information technology, HIPAA compliance, patient accounts, records, registration, and utilization management, among others.

**Gap Analysis and Risk Assessment**

Deployment of HIPAA technology solutions proceeds from an understanding of requirements, security risks, and potential weaknesses within the current security architecture. An assessment of the technology implications of HIPAA compliance should be conducted within the context of a broader examination of policies, procedures, and information flows. Any and all gateways to sensitive information must be safeguarded, but at the least, information systems must be scrutinized and upgraded to implement HIPAA standards, including EDI transactions, code sets, provider identifiers, patient privacy, digital signatures, data security, chain of trust, and more. A gap analysis will reveal deficiencies and potential threats to HIPAA compliance found in current systems and applications. A follow-up risk assessment examines alternative solutions, measured in terms of utility, impact, and cost.

From an IT perspective, a risk assessment must include a review of all systems and gateways through which sensitive data flow to evaluate
the risk of unauthorized access. This includes an examination of hardware and its accessibility, software and the sufficiency of applications-based access control, disaster contingency, and data flow mapping.

Beyond the IT angle, a risk assessment also includes an analysis of business and clinical operations from a process perspective, to determine what safeguards are in place to restrict access to sensitive information. Since HIPAA is not prescriptive, decision makers may select their own level of HIPAA remediation, as long as those decisions are reasonable and well documented. Some of the weaknesses that are discovered can be corrected by implementing IT solutions, but a greater proportion are not IT problems and must be corrected by tightening up physical processes.

Technology advances such as the Internet and the practical usage of portable transmission and storage devices (such as PDAs) raise additional issues concerning remote security of enterprise data. Finally, no information security scheme can succeed without the active compliance of staff. Employees must be educated, trained, and motivated to adopt practices that support the overarching goal of safeguarding sensitive information.

Strategy Development

HIPAA technology solutions are a component of a larger strategy that encompasses organizational workflows, policies, procedures — even culture. The HIPAA compliance team must consider the impact of technology, from the top of the house to every corner of their organization. More importantly, the team must integrate HIPAA compliance technology into a fabric of HIPAA policies and procedures that are drilled down to the department and functional levels. Ideally, a HIPAA compliance strategy will serve as more than a risk mitigator — it will serve as a catalyst of e-business activity, improve cash flow, and channel daily operations into more efficient venues.

To achieve this vision, the strategy must examine opportunities to digitize processes, create interoperability among devices and applications, and integrate systems. Finally, the strategy must consider issues such as security of mobile communications devices (such as cell phones and PDAs) and the adequacy of security architectures of third parties (such as vendors and trading partners).

Implementation and Maintenance

Like any technology installation, there are phases to a successful deployment including design, testing, installation, and refinement. A process must be employed to incrementally introduce these technologies, identify problem areas, define and execute solution sets, assign responsibilities, and create audit trails throughout the organization.

Additionally, there must be imbedded scalability into any technology solution that attempts to answer the HIPAA compliance demands of an organization, which is continually introducing new processes, applications, or business relationships.

The real HIPAA issue to be addressed is not data security alone but information security — it’s a process, legal, and operations issue as well. A reasoned assessment of information security strengths and weaknesses must include an investigation not only of IT processes but a review of risk management procedures, threats, and information flows across enterprise-wide operations — and beyond the organization. The ultimate challenge of selecting and deploying the correct information security architecture goes beyond functionality — it’s about executing a strategy that weaves together disparate computing systems within a single security framework, about compliance, about economic rationality, and about scaling your HIPAA technology solution for an information-intensive industry. Technology may not be the centerpiece of HIPAA remediation, but as healthcare gravitates towards digital information, it will increasingly permeate compliance solutions.

About the Author

Richard Krohn is president of Health Sense in Guyton, GA; rkrohn@health-sense.com.

References
