Securing e-Medical: A Primer on Protecting Health Information

Brian D. Handspicker, Engineering Director, Foliage Software Systems

Are *you* ready? With the HIPAA mandate for protecting health information nearly upon us, do the medical information systems you develop support HIPAA? Is your own environment secure enough to protect your customers? This paper provides a primer on security issues associated with developing, deploying, and supporting secure e-medical systems. This is the first in a series of papers from Foliage Software Systems discussing secure e-medical.

What is HIPAA?

"The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed into law by President Clinton on July 21, 1996. It has the general objectives to:

- Guarantee health insurance coverage of employees.
- Reduce health care fraud and abuse.
- Introduce/implement administrative simplifications in order to augment effectiveness and efficiency of the health care system in the United States.
- Protect the health information of individuals against access without consent or authorization."[1]

Health and Human Services (HHS) is responsible for developing the regulations that support and enforce HIPAA. Over the coming years HHS is expected to make rulings on aspects of HIPAA including how to: digitally encode health information, transfer health information over digital networks, and ensure the privacy and security of information. To date, HHS has published the following rules:

- Transactions and Code Sets (October 16, 2000, compliance October 16, 2002)
- Privacy (April 14, 2001, compliance April 14, 2003)
- Security and Electronic Signatures (proposed)
- Employer Identifiers (proposed)
- Healthcare Provider Identifiers (proposed)
- Healthplan Identifiers (proposed)

Note that compliance to each regulation is required 24 months after adoption for most organizations (36 months for small health plans). More information about the HIPAA act and the HHS regulations can be found at the HHS HIPAA website http://aspe.hhs.gov/admnsimp/index.htm.

[1] Security and Privacy: An Introduction to HIPAA, NEMA, April 10, 2001

Why is HIPAA important?

HIPAA was created in response to the need for the healthcare industry to reliably and confidentially exchange patient healthcare information in support of the portability of healthcare insurance and patients between employees, insurance companies and healthcare providers.

The HIPAA regulations defined to date provide neither the specifics of how they will be enforced – the Enforcement standard is not due until early 2002. However, civil penalties for HIPAA violations can include fines of up to $100 per incident with a maximum annual penalty of $250,000 per violation. And, criminal penalties for wrongful disclosure of protected health information can include fines up to $250,000 and/or 10 years in prison. Perhaps even more motivating is the prospect of aggressive civil court cases being brought by aggrieved parties when protected health information is disclosed without authorization.

With various HIPAA regulation deadlines approaching, it is important for all participants in the healthcare industry to evaluate the steps to supporting HIPAA compliance by Covered Entities.

Protected Health Information (PHI) is individually identifiable health information transmitted or maintained in any form, oral, written or electronic.

Covered Entities (CEs) formally include health plans, health care clearinghouses and healthcare providers. Covered Entities have regulatory responsibility for HIPAA compliance.

Business Associates (BAs) are external vendors and service providers that may have access to Protected Health Information on behalf of a Covered Entity. Medical device manufacturers and medical software vendors may be considered to be Business Associates if they have regular access to PHI through field service activity, product testing, or market research or joint medical research.

De-identification is the process of removing data from an individual protected health information (PHI) to ensure the privacy of a patient when that PHI must be exchanged between CEs that have no "need-to-know" the PHI.

Statistical Health Information is one means of de-identifying protected health information. For example, instead of sharing the raw information associated with a group of patients, the CE may share statistical information associated with the entire set. Care must be taken in deriving the statistical information to ensure that one cannot re-derive specific protected information about individuals through statistical analysis.

Non-interference with patient care is the over-riding requirement of any healthcare information system. In no case should the technology or policies supporting HIPAA compliance make information unavailable to authorized users. In addition, the electronic information must even be available in cases of power failures and equipment crashes. Finally, mechanisms must exist to allow healthcare professionals to over-ride security and privacy mechanisms in an emergency.

What does HIPAA mean to vendors?

HIPAA effectively shifts the regulatory burden of compliance from you and your products onto the healthcare institutions that are your customers. However, to market products in this new climate, the products must enable and support the customers' compliance efforts. In addition, medical device manufacturers and healthcare software vendors often find themselves in the position of needing to have access to their customers' protected health information to debug problems, perform proper field service, identify future product requirements and even support joint medical research. HIPAA characterizes the relationship between the vendor and their Covered Entity customer as Business Associates. This means that the vendor must ensure the same level of compliance to HIPAA and its associated regulations as their customers.

So, HIPAA presents a three-fold challenge to device and software vendors:

1. Incorporating necessary security technology into products to protect the privacy of the protected health information generated, managed and exchanged by the products at customer CE sites.
2. Re-evaluating and enhancing their own internal policies and training to ensure secure and confidential handling of protected health information exposed during testing, field services, product evaluation and research.
3. Supporting their customers in the creation of HIPAA-compliant workflows that incorporate their products, while at the same time ensuring that those resulting product-enabled workflows do not impede clinical communications or negatively effect patient care.

As most vendors have addressed Transaction Model and Code Set Requirements which become effective in just a couple of months, vendor attention is turning to regulations covering privacy of PHI and Security of Healthcare IT systems.

The “HIPAA Security and Electronic Signature Standards Notice of Proposed Rule Making” specifies the technical security measures that must be implemented by Covered Entities to properly secure Protected Health Information.

The “HIPAA Privacy Standards Notice of Proposed Rule Making” specifies patient's privacy rights and rules for how patient rights must be protected by Covered Entities. Protecting the privacy of electronic healthcare information requires ensuring only authorized people have access to the information, protecting the information from disclosure to unauthorized people, and controlling and tracking modification of the information.

To deliver products that enable and support HIPAA, there are a set of formal security and privacy practices and technologies that need to be incorporated into the products you deliver. In addition, being a HIPAA-compliant organization requires combining the security functionality that technology can provide with appropriate policies and procedures to ensure the effectiveness of the comprehensive privacy solution.

Medical device manufacturers and medical software vendors must now assess risks and develop, document, implement and maintain appropriate security measures to keep risk at an acceptable level. These measures include: administrative procedures, physical safeguards, technical security services and technical security mechanisms.

Of course, device and software vendors usually are not directly responsible for the organizational policies and procedures of their customers. But, their own policies and procedures must protect the confidentiality of information and their products can be developed to make it easier for CEs to comply with HIPAA. Specifically, HIPAA precisely specifies certain critical security policies and technologies, including:

- Unique IDs for authorized user
- Automatic logoff
- Audit trails for access to specific types of protected information
- Encryption (optional)
- Digital signatures (optional)
- Virus checking procedures
- Backup/Restore plans
- Disaster Recovery plans
- Compliance auditing
- Testing programs
- Training programs

How do I make my environment secure?

Delivering HIPAA-compliant security solutions requires more than just a few pieces of technology. To be effective, technical security solutions must be complemented by training, physical security, appropriate best practices-derived security policies and proper configuration of operating systems and applications.

Training: Training of both customers and internal personnel is a critical component of a comprehensive HIPAA-compliant security solution. The primary concern is ensuring that all users with access to Protected Health Information are sensitive to the patient’s right to privacy of that information. But, even personnel that are not authorized to have access to sensitive information must understand the importance of the privacy requirements of HIPAA. Since there are legal and regulatory ramifications associated with both authorized and unauthorized access, personnel must be sensitive to the patient’s rights and understand the policies and procedures implemented to secure those rights. Those policies and procedures are in place not only to provide protection of the patient’s rights, but also to provide legal protection to the personnel and their associated organizations.

Being open about how and where privacy is enforced helps users avoid becoming frustrated with “mysterious” lack of access. Far from improving privacy, “security through obscurity” often results in frustrated users attempting to subvert privacy via work-arounds. The weakest link in any security system is the humans that must have access to the protected information. Both authorized users and unauthorized users of a secure system need to understand what access the information systems will allow and why the constraints are in place. Properly secure technical systems will keep knowledgeable but unauthorized users from gaining access. But, only knowledge of and acceptance of privacy requirements will keep authorized users from improperly passing protected information to unauthorized associates. And, only knowledge of and acceptance of privacy enforcement will keep otherwise uninformed, and therefore frustrated, unauthorized users from requesting that protected information from their authorized associates.

Physical Environment: It's not sufficient to train your users well and deploy great technical security products. If anyone can walk into the Emergency Room, sit down at a logged-in workstation and gain access to secure data, your security measures have failed. The machines that generate secure information, that store that information and that process the information must be physically secure to prevent unauthorized users from subverting privacy by gaining physical access to the secure records. Physical security can range from simple locks on the doors, to high-tech biometric authentication scanners, to trusted human guards. The challenge is determining what level of physical security is necessary given the sensitivity of the information, the robustness of technical security, accessibility of the computing environment and trust-worthiness of the human staff.

Networks: Information being exchanged between distributed healthcare systems is exposed to potential discovery through various types of eavesdropping. Physical security of the networking components and communications media may be sufficient in small environments. In larger environments, and anytime protected health information is to be exchanged across a public network, the privacy of that information must be maintained through cryptographic and security technology.

Computer Operating Systems: Most modern computer operating systems provide sufficient security for protecting medical records. However, that security needs to be properly configured based on best-practices security policies. Configuration must include deleting unused and unnecessary user accounts, as well as ensuring that all passwords meet modern security requirements. Often computers or operating systems are shipped with non-secure, well-known user accounts configured for the convenience of the field service technicians installing the system (e.g. username="administrator", password="administrator"; username="guest", password="guest"). These are natural targets for unauthorized people and systems attempting to subvert security. In addition, many users have passwords that are either trivial to guess, easy to discover through password cracking programs or simply written on a Post-it note stuck to a monitor. A properly secure operating system must include both proper configuration to remove security holes and proper policies to ensure the users themselves don't open new security holes.

Application Software: As with operating systems, most modern applications have the potential to be configured for secure use. However, as with operating systems, most applications are configured by default to have very weak or non-existent security (e.g. DBMS systems with well-known default username/password pairs). Each application must be configured for secure use.

Data: Many types of information can be read by multiple different applications (e.g. image files). Relying solely on application-based security to protect the privacy of information will fail if unauthorized users can simply turn to a different less-protective application to read the information. Access control must be applied at the most fundamental level (files, database, etc.) in which the information is stored. In addition, in the case of information stored in databases, security must be applied at a minimum at the level of individual records. In some cases, database information may also need to be protected through some form of access control on the individual fields within records.

How do I make my products secure?

Of course, delivering products that support HIPAA compliance does require vendors to exploit security technology in their products. These technologies include:

Authentication: Authentication is the process of verifying the identity of a potential user of a system. At its simplest, authentication is performed through the verification of an access code or a username/password pair entered by the user at the time they wish access to the system. More sophisticated authentication mechanisms include the use of “smart cards” to store encrypted credentials and even biometric analysis of fingerprints, face-scans or retina-scans. Authentication on its own does not provide authorization to access any information or services provided by the system. Authentication only verifies that you are who you claim to be.

When an authentication attempt fails (e.g. an incorrect password is given), the attempt to access the system or information must be blocked and the failed attempt logged for future forensics investigation. A retry policy may allow the user to reattempt authentication. However, such policies must limit the number of retries and error messages should not provide any information that might be used to improve attempts to break into a system (e.g. never reveal whether it was the username or the password that was incorrect during a failed login attempt).

When a successfully authenticated session has been idle for a significant period of time (as specified by local security policy), then access to the session should be blocked and displayed information cleared from the screen until the user has successfully re-authenticated.

Technology supporting Authentication for PHI:

- Basic Authentication (Username/Password)
- Smart Card-based Authentication
- Biometric Authentication
- Digest Authentication
- Digital Certificates
- Notary/Verification Services

Authorization: Authorization is the process of determining what application and/or services an authenticated user is allowed to access. Authorization requires the matching of an authenticated identity, and sometimes an associated role (e.g. “administrator,” “owner”), with a list of applications, services or data that the identified user can use. The authorization can be determined by a simple match between identity/role and a specific right, or may involve a more sophisticated authorization rules service. Authorization to access specific data is sometimes also called “access control.”

Access control: Access control is the process of determining what data a user may read, modify, delete, or in some cases, execute. The specific type of access to which specific information can only be granted to a properly authenticated, authorized user with appropriate levels of access (e.g. a physician may have complete access to their own patient's information, yet only have access to de-identified or statistical information about another physician's patients). Obviously, care should be taken when granting access to not only preclude access to the unauthorized but also support access to information to a covering healthcare provider during appropriate periods of time.

Technology supporting Authorization and Access Control for PHI:

- Rules-based Access Control Tools (e.g. SiteMinder)
- Role-based Access Control Tools (e.g. Access Control Lists)

Accountability: Users of protected health information (whether authorized or not) are accountable for all access to, modifications to and distribution of that information. The HIPAA privacy regulation requires that unauthorized access to protected health information be reported. Audit logs are tools for logging the authorized and unauthorized use of the applications and/or services of a system as well as access and/or changes to protected health information. Regular inspection of audit logs is critical to protecting the security of the system, the integrity of protected information, and the legal standing of the organization.

Integrity: Protected health information must be represented, stored and distributed in such a way that any attempt to alter the information (whether authorized or not) can be identified and tracked. Typically a system-independent mechanism bound tightly to the information (e.g. checksum, CRC or digital signature) provides corroboration of the integrity of the information.

Non-repudiation: Non-repudiation takes integrity of information one step further to provide non-refutable evidence of creation, deletion, modification or distribution of information. This ensures that even an authorized user cannot access, change or share the information and then deny the access.

Technology supporting Accountability, Integrity, Non-repudiation for PHI:

- Checksums
- CRC (Cyclical Redundancy Checks)
- Double Keying
- Message Digests and Hash Functions
- Message Authentication Codes
- Digital Signatures
- Digital Timestamps

Confidentiality: Data in a secure system, or data being exchanged across secure distributed systems must not be viewable by unauthorized users or systems. Privacy often must extend to privacy of requests to the secure system. Unauthorized users could glean important information about data on the system simply based on "over-hearing" a request regarding the data (e.g. "copy fredsmith-hiv-test.doc.\archive").

Technology supporting Confidentiality for PHI:

- Private Key Encryption (e.g. DES)
- Public Key Encryption (e.g. RSA)
- Session Keys
- Message Integrity
- Replay Protection
- Key Management (e.g. PKI)

What do I do Monday morning?

Putting this information all together, medical device manufacturers and healthcare software vendors need to go through the following steps to ensure they provide proper support for HIPAA in their products and organizations:

1. Identify Potential Risks in Products and Policies
2. Develop Security Responses
3. Define Supporting Security Policies
4. Integrate Security Mechanisms into Products
5. Monitor and Audit Products to Identify Weaknesses
6. Repeat as Necessary

About Foliage Software Systems

Foliage Software Systems delivers custom software and systems integration services. Since being founded in 1991, Foliage has completed more than 150 projects for clients in healthcare, financial services, semiconductors, wireless services, avionics, and e-business. More than 75% of Foliage's 100 software engineers have ten or more years of experience. A 95% employee retention rate facilitates teamwork and continuity from project to project. Foliage has been consistently profitable, is self-funded, and has annual revenue of more than $25 million. Foliage is headquartered in Burlington, Massachusetts, and has a development and sales center in Campbell, California. Learn more about Foliage's track record by selecting from more than 90 case studies at www.foliage.com/medical.

Foliage
SOFTWARE SYSTEMS

Headquarters: 168 Middlesex Turnpike, Burlington, MA 01803 (781) 993-5500
Silicon Valley: 51 East Campbell Avenue, Campbell, CA 95008 (408) 321-8444