

Enabling HIPAA Compliant Patient Care



Introduction

The “Administration Simplification” provisions of the Health Insurance Portability & Accountability Act (HIPAA) mandate secure and private access to protected health information. They also seek efficiency improvements in the health care industry through standardized data transactions. Protected health information includes almost all identifiable health records and data that can be transmitted or maintained in any format. Guidelines have been issued that impose timelines for implementing HIPAA objectives by all covered health entities.

There are basically four areas of concern in the “Administration Simplification” provisions: privacy, standardized electronic transactions and code sets, security, and identifiers.

Privacy refers to the establishment of policy to restrict access, and identifiers provide for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system. As they do not directly call for a technical solution they will not be addressed in this paper.

“Electronic transactions and code sets” and “security” are areas that 3e Technologies International (3eTI) can assist with. A forward-thinking, young company, with strong engineering background in the development of secure systems and tools for data management, 3eTI provides solutions to HIPAA requirements by providing highly secure wireless networks and message translation software.

HIPAA Requirements Overview

HIPAA (as covered in 45 CFR parts 160,162, and 164) has sounded a wake-up call throughout the health care industry: Patient data is an asset and needs to be protected. HIPAA aims to improve the efficiency and effectiveness of the health care system, while increasing the confidentiality of individually identifiable health information.

The two HIPAA “Administration Simplification” provisions addressed in this paper are summarized in the following sections.

Transaction and Code Sets

By creating standardized electronic data interchange (EDI) transaction formats and code sets, HIPAA aims to dramatically improve operating efficiency in the health care industry. However, large entities already have major investments in their current data formats. The HIPAA requirement could force costly rewrite of their legacy IT systems and data records, as well as burdensome retraining of health care workers who use these systems. It requires a technical solution to minimize the short-term costs while achieving the projected long term benefits.

Security

Patient medical records are among the most sensitive of consumer data, since they can impact family financial as well as personal decisions. For example, many consumers with pre-existing medical conditions worry about the portability of their insurance or about potential employment. While the privacy provision is primarily a set of policy dictates with no technical component, it demands a robust technical solution to be effective. The security provision defines the technical standards both for safeguarding medical data transaction and for storage, which are required to adhere to the privacy dictates and prevent unauthorized viewing of sensitive information as well as to prevent fraud in conducting financial transactions.

Who is affected?

All health care entities are affected by HIPAA regulations. Health plans (over 3000 of them)¹ and health care

clearinghouses must comply with all requirements. While health care providers are not required under the existing regulation to change their administrative forms, if they choose to engage in electronic data transactions they must comply with HIPAA transaction format and code set standards. Complying with the administrative requirements would greatly reduce cost not only for transacting data with required partners (health plans) but also for internal administrative efficiencies. All covered health care entities must comply with privacy and security precepts.

Wireless Local Area Networks (WLANs) present a tremendous opportunity for hospitals and health providers, because patient information can be continually updated as patient care is administered and medical care activities can be monitored in real-time. With some 7,000 patient records of 50-300 pages in length found in the average primary care physician’s office², it is obvious how the use of an integrated patient care solution based on a highly secure wireless network can help to reduce costs, enhance efficiency, improve profitability, and ensure patient confidentiality.

Deadlines for compliance are illustrated in the following chart. Failing to meet requirements by the stated dates may result in fines up to \$25,000.

October 16, 2003	Electronic Health Care Transactions and Code Sets – all covered entities who filed for an extension and small health plans.
October 16, 2003	Medicare will only accept paper claims under limited circumstances.
April 14, 2004	Privacy – small health plans.
July 30, 2004	Employer Identifier Standard – all covered entities except small health plans.
April 21, 2005	Security Standards –all covered entities except small health plans.
August 1, 2006	Employer Identifier Standard – small health plans.
April 21, 2006	Security Standards – small health plans.

Source: Centers for Medicare and Medicaid Service

3eTI – the only WLAN vendor who can provide so comprehensive a solution

3eTI can significantly improve a healthcare entity's efficiency while ensuring it complies with HIPAA requirements in the areas of standardized transactions and security. For years, 3eTI has been at the forefront of development in both WLANs and applications for communicating among various software applications in an enterprise environment. 3eTI has the capability to translate messages from systems and devices across a network to usable formats for recipient devices and systems, including HIPAA compliant formats. These capabilities, combined with unmatched experience in WLAN security — in the most security sensitive market sector: the U.S. Department of Defense — create a solution set with unmatched potential to deliver the promise of wireless to the health care industry.

3eTI's solution to HIPAA's Transaction Format and Code Set requirements

The Problem — Currently, the health care industry is characterized by diversity of application and data format requirements. Preliminary attempts to standardize brought such numerous protests that no mandate to change the data collection instruments currently in use could be decided upon.

Message Manager as solution — 3eTI's Message Manager software application is a universal messaging system that enables communication among various software applications in an enterprise environment. It allows messages from devices and software applications across the network to be transmitted to other devices and systems where and when they are needed to support efficient business processes. For example, when a medical emergency is detected such as code blue, a doctor could receive a signal along with information about the emergency and the specific patient's records that prepare the provider to respond immediately to the situation.

Session Manager has three major components: data publishers, which receive transactions from legacy systems or devices; data subscribers, which receive transactions from Message Manager; and data topics, which are the message format. Message Manager dynamically assigns published messages to an appropriate data topic at the time the message is published. XML is used to structure data topics.

Security is maintained among the publishers by associating each data topic with a list of subscriber access rights assigned to that particular data topic. Message Manager will check access rights before allowing access to the data.

In the LAN mode, Message Manager is responsible for receiving and registering transaction requests (publish and subscribe) from various enterprise systems for specified data topics. It can be configured to help a health care entity translate its data into the HIPAA data format and assist with Electronic Data Interchange.

Standardized Electronic Health Care Data Transaction and Code Sets

Standardized data transaction formats and code sets are required to participate in the

overall HIPAA system. Translating legacy data could be burdensome and costly for entities with a major investment in legacy health record and transaction enterprise systems and devices.

By implementing 3eTI's Message Manager messaging and data translation software application, health entities can avoid costly reformatting of the data standards for transaction across their network to message recipients. The translation, once mapped into Message Manager, is performed as the data is transacted. Essentially, Message Manager is a program that can translate data fields to match the required output.

Electronic Data Transaction using Electronic Data Interchange (EDI) — Currently, information that is passed from one system to another must often be manually re-keyed, costing a lot of additional time.

3eTI's Message Manager can prepare the data formats and store them in a central, pre-formatted database, ready for transmission at a predetermined time to the external transaction partner.

The benefits of Message Manager — In short, use of 3eTI's Message Manager will simplify matching of legacy data and new data input for all sectors of the health care industry and allow efficient translation of data into formats required by the HIPAA legislation.

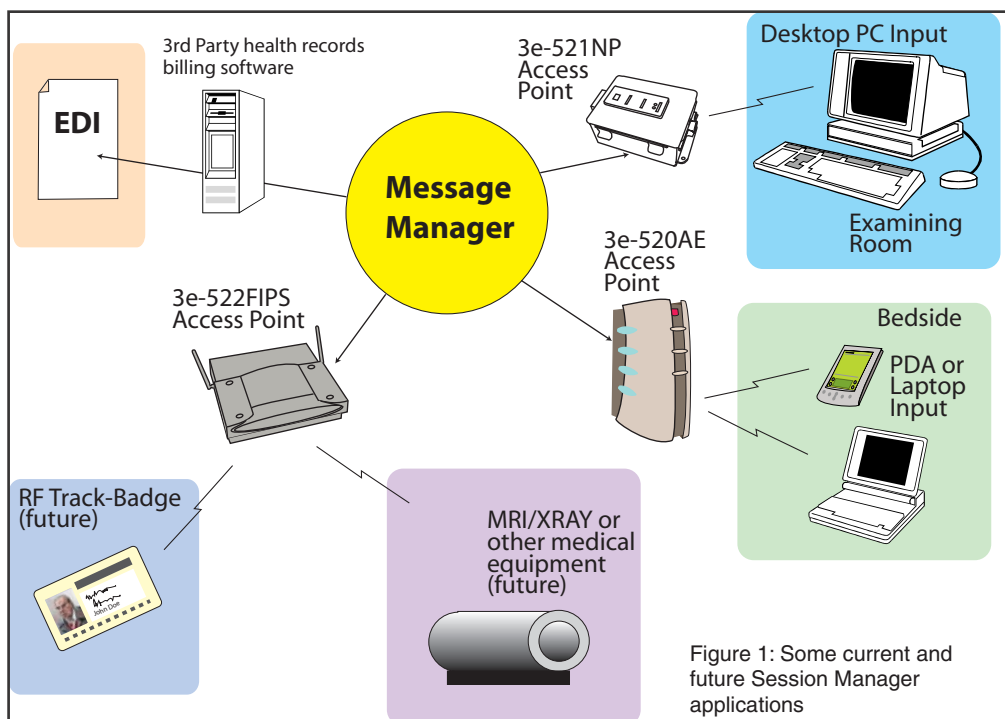


Figure 1: Some current and future Session Manager applications

3eTI's solution to HIPAA Security requirements

The traditional problems with wireless LANs

While wireless LANs (WLANs) are ideal for the health-care industry, difficulties with the traditional Wired Equivalent Privacy encryption algorithm (WEP) made businesses reluctant to employ WLANs. Transmitted data is broadcast over the air using radio waves. Because radio waves travel through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors or even outside the building.

Federal Information Processing Standard 140-2 (FIPS 140-2) is a standard, published by the National Institute of Standards and Technology (NIST), which describes U.S. Federal Government requirements for IT products to meet Sensitive but Unclassified use. FIPS 140-2 evaluation is required for any wireless products that are sold to the U.S. Federal Government.

3e Technologies International meets U.S. Government and Enterprise requirements for the highest levels of security by providing a FIPS 140-2 prevalidated, high-performance WLAN end-to-end solution.

3eTI's secure WLAN solution

The 3e WLAN Security Suite, employs the new, highly secure Advanced Encryption Standard, developed at the instigation of the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce and adopted as the standard for use by U.S. Government agencies. The 3eTI solution fulfills the need for a secure mobile networking solution.

The Security Suite can employ one of several models of access point (AP), a wireless PC Card that is compatible with the high security standard, and even a secure server which authenticates clients on the wireless network by distributing per-session secure keys enabling even greater security. In addition, each AP has variable radio frequency (RF) management capability, allowing it to be programmed to meet the particular environment. All APs can be configured to use Power over Ethernet (PoE), reducing even further the need for cabling, as the power is delivered over the Ethernet cable rather than being plugged into a power outlet with a power cable.

Configured by 3eTI professionals into an integrated wireless LAN to meet the needs of a particular healthcare entity, the 3e WLAN Security Suite provides greater freedom and efficiency than was possible under traditional wired LANs and meets the highest security standards.

The following paragraphs describe the components of the 3e WLAN Security Suite.

The access point — There are three access points that meet the requisite level of security. Two are contained in rugged water-resistant metal enclosures, made to withstand the rigors of industrial environments. One is in an aluminum box and is thus non-magnetic while the other is in a steel enclosure. The third AP has removable (and thus upgradeable) antennas and a more "office-compatible" look. All three contain the cryptographic module that has passed independent lab testing for FIPS 140-2 Level 2 compliance and which is in the process of NIST certification. All three



can be configured to use Power over Ethernet, eliminating an additional power cable.

The client software and PC Card — The 3e-110 WLAN PC card and its 3e-010F Crypto Client software provide advanced wireless radio frequency (RF) data security with AES or 3DES (an alternate standard that is also approved) encryption. The 3e-110 WLAN PC Card is an 802.11b Extended Range card. The 3e-010F installation and utility can be purchased separately so that, if the entity already has compatible wireless cards using the INTERSIL PRISM 2 or 2.5 chipset, these can be used with the additional secure installation.

RF Management — Each AP incorporates RF Management. This means that the radio frequency broadcast by the APs can be managed, either singly or as a group, to comply with the needs of the specific environment. For example, if the AP signal needs to broadcast over a wide range, the RF will be turned up. If wide broadcast results in competing APs, the RF can be turned down. In dense urban exterior or interior environments, the power may need to be managed to prevent broadcasting too widely.

The 3e-030 Security Server software — The 3e-030 Security Server software, if purchased, resides on a separate network computer and creates, distributes and manages "dynamic" per-session keys for each user, each time they log into the network. It also authenticates each user by distributing and managing their certificates. AES or 3DES encryption alone is sufficient for many security needs, but, as they employ a static key, the use of the 3e-030 Security Server provides the ultimate in security.

How 3eTI's solution helps meet HIPAA's Security requirements

HIPAA has established requirements for unique user identification, encryption, audit controls, integrity, person or entity authentication, and transmission security. The 3e WLAN Security Suite can help you meet HIPAA's requirements.

Unique User Identification — HIPAA requires that “electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 45 CFR 164.308(a)(4).”

By implementing 3eTI's strict security measures, only those people with legitimate access to a patient's health record can access it. 3eTI's solution includes X.509 Certificate Based Authentication, user authentication and MAC address filtering.

Encryption — HIPAA requires the entity to implement an encryption algorithm whenever possible, as stated: “Implement a mechanism to encrypt and decrypt electronic protected health information”.

The 3e WLAN Security Suite provides state-of-the-art encryption including AES and 3DES, both of which are FIPS 140-2 prevalidated as mandated by the U.S. Department of Defense.

Audit Controls — HIPAA requires implementation of mechanisms that record and examine activity in informa-

tion systems that contain or use electronic protected health information.

3eTI's Message Manager software module, employed with the 3e WLAN Security Suite, provides an audit trail of transactions.

Integrity — HIPAA mandates that the entity implement policies and procedures to protect electronic health information from improper alteration or destruction.

The 3e WLAN Security Suite provides unique user authentication, “dynamic” session specific keys, and creation/management of x.509 user certificate features. In addition, the WLAN can provide electronic backup of the health entity's records, a failsafe to ensure that health information is not lost.

Person or Entity Authentication — HIPAA requires user authentication.

Each unique WLAN user is stringently screened through highly secure 802.1x / EAP-TLS authentication routines. In addition, RSA based digital signatures are required to support dynamic key exchange.

Transmission Security — HIPAA demands transmission security.

Using the 3e WLAN Security Suite with its FIPS prevalidated AES / 3DES encryption ensures that all wireless data & records transmission is impervious to snooping by unauthorized persons and impenetrable to hacking.

Conclusion: a Healthcare Opportunity

3eTI's Message Manager software can translate data formats from legacy systems and devices into a HIPAA compliant transaction format. It can simultaneously connect the disparate devices across a network, using both wireless and wired connections, and collect their data inputs to be stored in central, HIPAA compliant record-keeping databases for later transmission when and where it is needed for efficient business processes to external entities. The “Administration Simplification” section of HIPAA envisions dramatic improvement in the efficiency of the US health care system through implementation of its provisions estimated worth billions of dollars, provided their implementation can be made less painful in the short term.³

With the use of 3eTI's WLANs, healthcare staff can access highly secure, real-time patient information without being tethered to a hardwired port. The mobility offered by a wireless networking solution permits vital information to be accessible anytime, anywhere – where the data is needed. This flexibility improves delivery of patient care, streamlines workflow, and reduces cycle time to update/maintain records. For example, nurses can move from room to room providing medication and care while being connected to the patient's medical record. Caregivers can access and update patient files in real time. Interns and residents can retrieve updated patient information when they come on duty by synchronizing their PDA to the clinical database. They can receive their patient lists and key test results. They can even receive and view X-ray images on the PDA screen.

3e Technologies International has long been in the forefront in the development of secure wireless and data networking solutions. 3eTI's staff of experienced engineers can work with the healthcare industry to develop uses that meet HIPAA needs while implementing new, more efficient and secure solutions.

Footnotes

¹ Final Rule and Notice, Federal Register vol.65, no. 160, Aug 17, 2000, p. 50358

² Advance News Magazine: Health Information Professional. March 2002.

³ Final Rule and Notice, Federal Register vol.65, no. 160, Aug 17, 2000, p. 50358