

Standardizing Communication and Encryption in the HIPAA Environment

by
Daniel I Kazzaz
Rapid Data Integration, LLC

Now that we are all speaking the same language...Can you hear me?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), contains provisions designed to reduce health care administrative costs. HIPAA mandates that all payers and providers be able to exchange electronic administrative messages including claims, authorizations, eligibility verification, etc. in a common format. This is a huge leap over today's Tower of Babel mode where every organization sets their own data rules. Even with standardized messages, the healthcare industry will not be able to exchange data smoothly unless both data communication and encryption standards are set and followed. Fortunately, healthcare does not need to create a new standard; AS1 already exists and is becoming increasingly popular in corporate America.

Background

Electronic communication between payers and providers has existed for decades. Large payers interact with tens of thousands of physicians and group practices. Most payers have invested heavily in automated systems to facilitate data processing.

Additionally, payers have invested in assisting providers automate the submission of electronic claims by providing some combination of software, hardware and communication lines. Payers, however, are not the only ones with a vested interest in communicating with providers. Clinical laboratories (for blood testing), pharmaceutical companies, State Health Departments and medical supply companies have similar needs. With little or no cooperation between the interested parties, each group has invested in providing healthcare providers a separate "no cost" path to their system. The net result is that most provider entities have some hodgepodge of software, hardware and phone lines that they must support solely for communication with other parties.

There have been several attempts designed to reduce the clutter in the provider office. These solutions have been called Health Information Networks (HIN's). Most of these have met with only limited success. Typically, networks that gain their revenue from claim traffic could not justify the expense to support clinical pathways. Similarly, clinical pathways could not truly co-reside with administrative ones.

The late 90's led to several new attempts to create dot-coms to connect providers to payers and other entities. In general, these dot-coms were focused on satisfying only one market need, either billing, exchanging medical records or ordering supplies. Until now, everyone has avoided the simple step of using encrypted email to securely transport industry standard messages.

Moving Data from A to B

Every year brings a new technology to move data between computers. The technologies fall into three general categories: physical media, wired technologies and wireless technologies. Healthcare organizations, for their inter-organizational communication, use both physical media and wired technologies.

Physical Media

The earliest exchanges of information between computers used punch cards. These were thin cardboard sheets with 12 rows and 80 columns. To move data from one computer to another, the cards were punched by one computer then read by another. This method was inefficient and wasted resources and was quickly replaced with magnetic media.

The first popular magnetic media solution was reel-to-reel magnetic tape. These tapes held a great deal of data and were reusable. Assimilating tapes created by outside organizations was always difficult. Reading tapes was problematic because neither the tape drives nor the data format were standardized. Even though some Medicaid processors only recently stopped using this technology as the sole method of moving data, most entities have not exchanged tapes for quite some time.

With the personal computer (PC) revolution, diskettes became a popular medium of exchange. A single 3½ diskette held 1.4 million bytes of data, which is as much information as 17,500 punch cards. Data movement from PC to PC inside or outside the organization was trivial. This media was light and easy to ship. The 5¼-inch and 3½-inch diskettes evolved into the de-facto standard for backups, software distribution and data exchange. They remained there until the laser (compact) disks appeared on the scene.

Today, Compact Disk (CD/DVD) writing technology is readily available. Some formats are erasable and others are not. The reusability is not an issue because large amounts of data can be stored, shipped and retrieved on each CD/DVD. A CD holds 500 million bytes of information. A DVD holds 10 times more.

Exchanging data via physical media, whether it is paper or diskette, requires manual intervention at both ends. Many payers send and receive information on a daily basis from tens of thousands of providers. Manual intervention adds unnecessary overhead expenses. The only practical solution is to exchange data via wired or wireless technologies.

Wired technologies

Dial-up

Early computers were not capable of connecting to each other. These computers had serial ports wired to computer terminals. They were designed with the expectation that data entry and programming were done on each terminal. Connecting the serial ports of different computers and emulating the expected typing accomplished the first networking of computers.

The serial ports could also be connected to modems, which were then connected to phone lines. Outside users could connect their terminals or computers to modems and phone lines to dial-up the computer. This function is called Asynchronous or Dial Up connectivity.

Implementing Asynchronous connectivity requires creating systems called electronic bulletin board systems (BBS). These BBS computers listened to phone lines and the connecting systems would dial-up. The operations staff of the listening computer established user id's, passwords and a dialogue for logins and file transfers. Similarly, the dial-up users would have to program their dialers for each listener's specific prompts. Since the transfer of information was accomplished by simulating keystrokes and the communication was often over "noisy" telephone lines, data was often dropped. As a result, data checking protocols (Kermit, Xmodem, Ymodem) were developed to safeguard the information.

Asynchronous/Dial-Up is the technology used for dialing into the Internet from home, office or mobile device. The underlying technology of using a serial port and a modem remains the same. Fortunately, the dialogues and the protocols have been standardized.

Leased Lines

Hospitals, Clearing Houses and Payers frequently connect to one another with leased lines. The lines are needed for higher throughput (bits per second) and tighter security. Providers are often told to use leased lines to connect to certain payers because it is the only way to inquire on the status of their payment (claim status inquiry).

Leased lines are expensive and difficult to support. Most non-healthcare companies have transitioned away from leased lines to connect to each other; they use encryption over the Internet.

HUB-Spoke vs. Peer-to-Peer

Looking at the world from a hardware perspective, the only way to establish global connectivity is to devise a hub-spoke environment by wiring groups of lines to switches. These switches are then connected to other switches to allow for point-to-point dialogues. As long as a standard exists, any spoke on any switch could communicate with any other. From a telephony perspective, each phone line is a spoke and the phone companies are the hubs. The phone companies can connect their switches to each other on a peer-to-peer basis. Peer-to-peer capability means that either side can push or pull information. Solving the communication challenges in healthcare requires that it move in that direction.

Initially, hub-spoke based systems were the only way for companies to interconnect. Large companies (payers) would be hubs and set up listening technology. The smaller entities (providers) would be the spokes and set up the automated dialup. The large company manages thousands of connections. The only possible way for a large company to manage this many connections was for them to set up a unified listener protocol. As no standard exists for this in Healthcare, the smaller companies (spokes) are forced to tailor their systems to the large companies of importance. It is not possible for the provider to tailor their communication scripts for all the payers.

The lack of standards is not the only drawback for Hub-Spoke methodology. Hub-Spoke technology impedes Hub-Hub and Spoke-Spoke communication. In fact, each hub tends to be so unique that it cannot support automated communication with spokes not specifically configured. Healthcare connectivity must be standardized and simplified. This can be accomplished by implementing a standard based peer-to-peer protocol.

Clearinghouses

There are approximately 600,000 provider groups and 6,000 different payers in the US. It is nearly impossible to truly connect every organization to each other. Networks of clearinghouses are in place to help provide the needed linkages. These service bureaus also provide data tracking, data cleansing and data conversion services.

Claims clearinghouses fall short in several key areas – they do not support clinical connectivity, they do not support *all* the HIPAA transaction sets and they do not provide universal connectivity. (One cannot reach all providers or payers from each clearinghouse). They can easily make up for these deficiencies by standardizing on communication.

Moving Data on the Internet

The Internet is not just a series of connected computers; it is also a set of standards. Because everyone uses the same standard we can send email each other knowing only an email address. We can browse web sites on any computer. We do not need to know the brand of computer, web sever or email package that sits at the other end. There are 3 standards supporting this activity:

1. HTTP – Hyper Text Transport Protocol is the methodology by which HTML (Hyper Text Mark Up) pages are retrieved by browsers. Clicking on an icon to take us to a web page, we are, in reality, downloading a file.
2. SMTP (Simple Mail Transport Protocol) is the protocol that allows us to email each other. Files are sent to each other as attachments.
3. FTP (File Transport Protocol) is a method to move larger files.

The HTTP and FTP protocols are hub-spoke protocols. A spoke needs to initiate contact and deal with hub specific rules for logins, file names, etc. SMTP is a peer-to-peer protocol. With SMTP either side can initiate the transfer of information.

Encryption

Internet data travels in the clear and is easy to intercept. In order to keep data private it must be encrypted before it is routed through the Internet

There are many ways to move information securely. The Data Encryption Standard (DES) is the most commonly used algorithm to encrypt and decrypt data. This standard relies on a shared key between sender and receiver. It is a highly efficient algorithm, but requires frequent key changes for protection.

The RSA algorithm uses the public key / private key pair (PKI) concept. You create both keys, keep the private key secret and publish your public key. Only the matching private key can decrypt data encrypted with its corresponding public key (and vice versa). Anyone can use your public key to encode data that only you can decode. Data successfully decoded with your public key can only have been encoded with your private key. This is why data signed (encrypted) by a sender's secure private key establishes non-repudiation.

Many implementations combine RSA and DES by using RSA to exchange a “session key” and using that session key to uniquely encrypt the traffic. The public key and private key approach is the easiest to manage. As long as the private key is stored securely, the corresponding public key can remain unchanged.

Organizations need to exchange public keys with the companies they communicate with. Many believe that a certification authority is needed to maintain, certify and distribute these public keys. Others believe that simpler methods would suffice.

Combining Data Moving Standards with Encryption standards

There have been many attempts to move data securely on the Internet. The most common method is called Secure Socket Layer (SSL). This technology is used within secure Web access (HTTPS). Quite frequently, organizations establish SSL connectivity and then move files within this arena. (The challenge with this approach is that it is hub-spoke based rather than peer-to-peer.)

There is a standard for moving data securely on the Internet that combines encryption and email. The standard allows data to be encrypted and sent as an email attachment. This standard, called AS1 or EDIINT, was developed in the early days of the Internet to facilitate corporate to corporate electronic commerce. The early adopters were surprised by the ease of implementation and reduced transmission times.

The AS1 standard adoption has been industry by industry. The earliest implementers were banks, followed by shipping companies. The largest retailers are now using it to communicate with their suppliers. The reason this technology is so appealing is that it is extensible. It is peer-to-peer, it relies on pervasive technology and it is inexpensive.

Government guidelines

The CMS Internet Communications Security and Appropriate Use Policy and Guidelines can be retrieved from http://www.cms.hhs.gov/it/security/docs/internet_policy.pdf. The position of the Federal Government is encapsulated in the following quote from this policy statement.

“In summary, a complete Internet communications implementation must include adequate encryption, employment of authentication or identification of communications partners, and a management scheme to incorporate effective password/key management systems.”

The standard AS1 meets these criteria. AS1 includes Secure Multipurpose Internet Mail Extensions (S/MIME) based transport mechanism which uses the private / public key pairs for both encryption and authentication. The commercial software packages supporting AS1 include password and key management subsystems.

Advantages and Disadvantages

Method	Advantages	Disadvantages
Physical Media	<ul style="list-style-type: none"> <input type="checkbox"/> Most secure. <input type="checkbox"/> Cost per byte transferred is very low. <input type="checkbox"/> Peer-to-peer. 	<ul style="list-style-type: none"> <input type="checkbox"/> Manual intervention required for creation, sending, tracking and receiving. <input type="checkbox"/> Physical media types become obsolete every few years.
Dial Up	<ul style="list-style-type: none"> <input type="checkbox"/> Inexpensive when all connections are local and modem speeds are fast. 	<ul style="list-style-type: none"> <input type="checkbox"/> Requires multiple protocols – Xmodem, Ymodem etc. <input type="checkbox"/> Proprietary scripting based on BBS software. <input type="checkbox"/> Password Protection and resetting is cumbersome. <input type="checkbox"/> Software vendors disappearing. <input type="checkbox"/> Hub-Spoke <input type="checkbox"/> Requires Multiple phone lines
Leased Line	<ul style="list-style-type: none"> <input type="checkbox"/> Secure guaranteed connection. <input type="checkbox"/> Peer-to-peer. 	<ul style="list-style-type: none"> <input type="checkbox"/> Very Expensive <input type="checkbox"/> Difficult to set up and maintain.
Clearing House / Van	<ul style="list-style-type: none"> <input type="checkbox"/> One setup can provide multiple connections. <input type="checkbox"/> Understand either regional or practice specialty requirements. 	<ul style="list-style-type: none"> <input type="checkbox"/> Hub-Spoke. <input type="checkbox"/> Single purpose (billing only). <input type="checkbox"/> Increasing cost based on volume. <input type="checkbox"/> Little or no support for ALL of the HIPAA transaction sets – in particular the interactive messages. <input type="checkbox"/> Many clearinghouses run on obsolete equipment, posing a possible liability.
SMTP	<ul style="list-style-type: none"> <input type="checkbox"/> Peer-to-peer. <input type="checkbox"/> Easy to implement. <input type="checkbox"/> No extra fees to phone company 	<ul style="list-style-type: none"> <input type="checkbox"/> Has attachment size limitations. <input type="checkbox"/> Healthcare data must be encrypted
HTTP	<ul style="list-style-type: none"> <input type="checkbox"/> Easy for HUB to implement. <input type="checkbox"/> Can establish secure connection with HTTPS. <input type="checkbox"/> Can support Interactive <input type="checkbox"/> No extra fees to phone company 	<ul style="list-style-type: none"> <input type="checkbox"/> Proprietary scripting or package is needed. <input type="checkbox"/> Hub-Spoke. <input type="checkbox"/> Setup is challenging for interactive. <input type="checkbox"/> Password Protection and resetting is cumbersome
FTP	<ul style="list-style-type: none"> <input type="checkbox"/> Easy for HUB to implement. <input type="checkbox"/> Can support very large files. <input type="checkbox"/> No extra fees to phone company 	<ul style="list-style-type: none"> <input type="checkbox"/> Batch only <input type="checkbox"/> Healthcare data must be encrypted <input type="checkbox"/> Proprietary scripting or package is needed <input type="checkbox"/> Hub-Spoke

Upcoming Technologies

Some new technologies are available to move data from one place to another. These new data paths could drive down costs even more. These paths rely on the Internet standards to move data.

Broadband

The Cable Television Signals we receive in our homes are delivered with Broadband network support. Connecting to the Internet over either a Cable Modem or DSL modem over voice lines sits on Broadband technology. There is a large and growing residential use of broadband to establish Internet connections. As Broadband service improves, the uses of this technology in small businesses will take off. The small business owner will undoubtedly migrate to the lowest cost high-speed lines available.

Wireless

At their core, all wireless technologies -Walkie Talkie, Satellite transmission, FM radio, Pagers, cell phones, wireless LAN's and Wireless Fidelity (WIFI) - operate in a similar fashion. There are transmitters and receivers. Three important items determine its capabilities – the power of the transmitters; the sensitivity of the receivers and the coding of the signal. The coding of the signal allows a single pager to beep or phone to ring. The three coded technologies used in data exchange are satellite, cell phone, wireless LAN and WIFI.

Satellite technologies are used for both data and voice. Leasing bandwidth on satellites is expensive and using it for two-way communication is complex, limiting its use. The primary users are: the military, the phone companies, the news media and manufacturing plants in remote areas.

The digital cell phone is beginning to incorporate data as a regular payload. Today, many users connect their cell phones to their laptops for Internet access. Newer encoding methods will make it even easier to connect to the Internet using cell-based technology. It is not yet clear that the bandwidth (characters per second) on cell phones is high enough to accommodate today's appetites for data volume. Therefore it is likely that another technology, such as WIFI, will become the dominant wireless technology of the future.

Summary and recommendation

HIPAA implementations are forcing a wide range of changes in the Healthcare industry. While the data formats are being changed, there should also be a change in how data is moved. Rather than re-invent the wheel, impose some new proprietary methods or continue the chaos of multiple methods – Healthcare should adopt email based AS1 technology. This protocol meets Healthcare’s data moving requirements. Using an email-based technology will be a vast improvement over current dial-up and physical media methods of moving claims, orders and clinical data

The AS1 standard was proposed a decade ago as an Internet Engineering Task Force (IETF) standard. It is a proven technology, in use by several fortune 500 companies. An interoperability certification procedure for validating software packages has been in place for at least 8 years. There are already 16 commercial, off-the-shelf products certified as interoperable. There are many more on the way.

Patient Management System (PMS) software vendors are not supplying the healthcare provider community with HIPAA compliant EDI solutions. A large reason for this is that software vendors cannot afford to tackle the differing implementations required by each major insurance company. This lack of standardization increases means that providers must continue to submit claims, authorizations, attachments and many other messages on paper. The standardization of the communication and encryption protocols could prove to be the watershed event that will encourage the providers to switch to electronic communication with all payers. This move will save the Healthcare industry the billions of dollars.