Primer on Encryption

Save to myBoK

by Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

Encryption is an addressable implementation specification under HIPAA’s access control and transmission security standards. Many providers are grappling with just how to address these specifications:

- Is there a difference between the two specifications, and if so, what is the difference?
- Must encryption be used, and if so, what form of encryption should be used?
- If encryption is not used, what are appropriate alternatives?

Comparing Standards: Access Control versus Transmission Security

The access control standard relates to data at rest; that is, data stored in electronic form. This storage may be a computer’s main memory, other forms of memory, or secondary storage. Secondary storage may or may not be connected to, or a component of, a computer at any given time.

All forms of storage must be considered because the range of electronic media that stores data—even temporarily—is continuously expanding. For example, personal digital assistants (PDAs), mobile telephones, notebook and tablet PCs, smart cards, and flash drives and memory sticks have the potential to store protected health information (PHI) and are becoming ever smaller, more portable, greater in capacity, and more universally compatible with other systems. Today, a flash drive can store as much data as a mainframe computer once did, can be carried on a key ring, and can be used on any computer that has a universal serial bus (USB) port. We can only speculate on the improved versatility of future devices.

The transmission security standard applies to data en route or in transit. Data may be transmitted through hardwire cables that are owned or leased, such as telephone wires, or radio and other wave forms. Each transport mechanism has its own level of security. Owned cable is generally considered more secure than telephone lines, and telephone and cable lines are more secure than wave forms.

Data are considered to be in transit when they are sent from point A to point B. When data are at point A or have reached point B they become data at rest. This distinction is made because the common belief is that data need to be better protected in transit rather than at rest. However, data actually spends little time in transit and most of its time at rest—even while the device in which it is resting may be moving around.

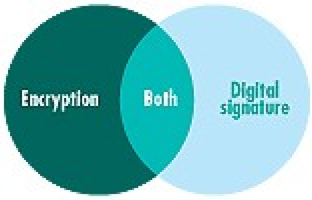
Consideration must be given to the storage and transport media used and their inherent security mechanisms, as well as the amount of time and volume of data spent at rest or in transit. For example, a clinical messaging system that uses a virtual private network (VPN) is probably more secure than a PDA that contains PHI and can be left in a restaurant or on a train.

Encryption: What It Is and How It Works

Encryption refers to the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Encryption transforms readable data (plain text) into a form that conceals the data’s original meaning to prevent it from being read or used (cipher text).

Encryption belongs to a class of processes known as cryptography. Cryptographic systems may provide encryption only, a digital signature only, or both encryption and a digital signature. (See “Cryptography Functions,” below.)

Cryptography Functions



A digital signature authenticates a message's sender. Encryption encodes the content. Cryptographic systems can provide either or both forms of security.

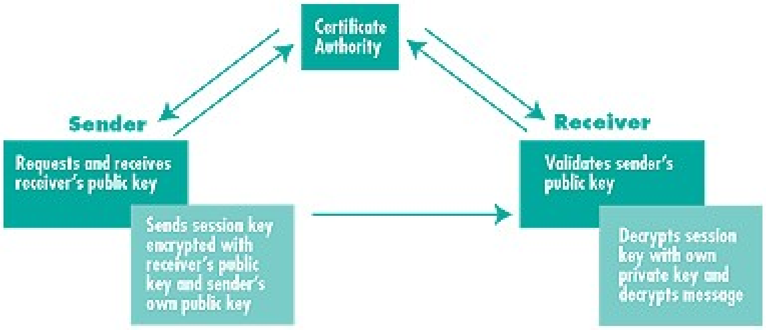
© 2004 Margret\A Consulting, LLC. Reprinted with permission.

A digital signature is a means to uniquely identify the sender of a message, verifying the origin and identity of the sender. (Note: the verification of origin and identity of the sender distinguishes a digital signature from an electronic signature, which is only accomplished through the use of an authentication control, such as a password, token, or biometric.) A digital signature uses a cryptographic process but only operates on the authentication aspect of the message, not the message content itself. To mask the message content, there must be encryption.

There are two main types of cryptography. Secret key or "symmetric" cryptography entails the exchange of a secret key with the party to whom an encrypted message is sent. So if Dr. A wants to send Dr. B an encrypted message using secret key cryptography, Dr. A must convey the secret key to Dr. B before or after sending the message so that Dr. B may decrypt the message. From a practical standpoint, this means two communications when one is often desired. Additionally, unless the secret key is for one-time use or valid only for a specified period of time, Dr. B now has potential access to any data Dr. A encrypts. If Dr. A is lax about keeping the keys secure for all the various persons with whom there are such communications, Dr. B becomes a gold mine of secret keys.

The second form of cryptography, called public key or "asymmetric," overcomes the need for a secret key. Public key cryptography uses two keys: a public key and a private key. The public key is made available to anyone who wants to encrypt and send a message. Thus the need to exchange secret keys is eliminated. The process is illustrated in "Public Key Cryptography" below.

Public Key Cryptography


Certificate Authority
Sender
Requests and receives receiver's public key
Sends session key encrypted with receiver's public key and sender's own public key
Receiver
Validates sender's public key
Decrypts session key with own private key and decrypts message

© 2004 Margret\A Consulting, LLC. Reprinted with permission.

Although the public key cryptography process appears complicated and time-consuming, once the certification process has taken place, the sender and receiver are able to communicate in a secure manner on an ongoing basis.

Encryption Alternatives

In both types of cryptography, there are multiple algorithms. The algorithms use various sizes and formulas that determine the “strength” of the process; that is, how rapidly the cryptography can be broken using sophisticated processing methods. If a provider is only going to encrypt its own at-rest and in-transit data within its own circle of control, it is possible to settle on one standard and apply it universally. However, once the provider wants to transmit data outside that circle of control (such as with multiple payers, patients, or business associates), the single standard is no longer a solution. Each payer, patient, or business associate may have its own encryption or digital signature standards, in which case multiple standards need to be accommodated.

Many providers sidestep the issue of encryption and apply stronger access controls, audit trails, and authentication processes to data at rest and use transmission media that are inherently more secure. For example, to communicate with payers, many providers use a clearinghouse with which a secure transmission mode has been established. The clearinghouse then forwards the transactions to payers and other clearinghouses also using secure transmission modes.

Electronic communication between a hospital and physician office has generally been asynchronous—a message can be sent or received, but there is no ability to interact with the data in a communication session. E-communication between hospitals and physician offices are also physically limited to where such communication capability is provided.

Typically, physician offices have had the ability to view results or receive transcription, which was managed by routing the communication through a secure cable or leased line. More synchronous communications from multiple locations are needed. For example, a physician may want to receive a discharge medication list from the hospital, update it, and sign it as a discharge order in one communication session, as though the physician were right in the hospital. Such communications can be performed through cable or leased-line connections, but many physicians want to be able to connect from any location using the Internet.

Many providers are looking at secure Web portals through which such communication can take place securely as an alternative to encryption. This option is available for communications with patients. The cost of such portals is not cheap but may be less expensive than encryption when multiple forms must be managed.

Alternatives are also being considered for data at rest. Strong access controls, audit trails, and authentication are important, but most of these are still insufficient for data that are stored on portable media. Using these media as human-computer interfaces and not storing any data on the device is generally the best alternative unless a strong form of encryption can be applied. Many of the portable devices with wireless connectivity have the capability of wiping out data from cache memory when the device is physically moved out of the wireless access range.

***Margret Amatayakul** (margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "A Primer on Encryption." (HIPAA on the Job column), *Journal of AHIMA* 75, no.6 (June 2004): 52-53.