Connecting Healthcare®
Engaging Patients™

HIPAASuccess - Physician Education Series

Electronic Signatures

Your Faculty:
Walt Culbertson

- President and Founder, Connecting Healthcare®
- Host and Producer, Medical Update Show
- Served as Technical and Operations Lead, HIE Project Manager Florida Health Information Exchange
- Served as the State of Florida - Technical SME for the ONC State Health Policy Consortium, Southeast Regional HIT-HIE Collaboration (SERCH)
- Founding Executive Director ePrescribe Florida and President, ePrescribe America
- Founding Chair of the Southern Healthcare Administrative Regional Process (SHARP), a regional collaborative workgroup alliance of private and public health care organizations and HHS, HRSA and CMS
- Founding Co-Chair of the CMS Sponsored Southern Insurance Commissioner Task Force, a regional collaborative workgroup alliance for State-level HIPAA Education
- Founding Security and Privacy Co-Chair for the Workgroup for Electronic Data Interchange (WEDi) Strategic National Implementation Process (SNIP)

Electronic Signatures

- HIPAA directs the Secretary of the Department of Health and Human Services to coordinate with the Secretary of the Department of Commerce
  - In adopting standards for the electronic transmission and authentication of signatures with respect to the transactions referred to in the law
  - This rule was developed in coordination with the Department of Commerce's National Institute of Standards and Technology

Electronic Signatures

- Proposals for the use of e-signatures under HIPAA rules were included in the first draft of the 2003 Security Rule, but then removed before the legislation was enacted
- Generally, a signature is not required for many healthcare transactions that disclose PHI for treatment or payment

Electronic Signatures

- If deployed, the conditions necessary for e-signatures under HIPAA rules also have to take into account the Federal Electronic Signatures in Global and National Commerce Act (ESIGN Act) and the Uniform Electronic Transactions Act (UETA)
- It has been proposed that the industry adopt a cryptographically based digital signature as the standard.
  - As opposed to electronic signatures which is a digital scan of the pen based signature

Electronic Signature is Defined

- Most of the security requirements outlined in the final regulations are quite general, and the stated focus of the regulations is to be "technology neutral"

HIPAA Signature Requirements

The proposed Security rule specifies that if used an electronic signature must accomplish the following:

- Identify the signatory individual
- Assure the integrity of a document's content
- Provide for non-repudiation, which is strong and substantial evidence that will make it difficult for the signer to claim that the electronic representation is not valid

HIPAA and Encryption

- There is a great deal of debate about the use of encryption being a required technology based on the final HIPAA security rules
  - The HIPAA Security Rule requires “unique user identification” in accessing electronic protected health information (ePHI)
  - Leaves encryption as an “addressable” standard both in access controls and data transmission

Digital Signature

Requirement

[1] If digital signature is employed these must be implemented

Implementation

- Message Integrity [1]
- Non-repudiation [1]
- User Authentication [1]

Digital Signature

Requirement

[2] These features are optional even if Digital Signature is utilized

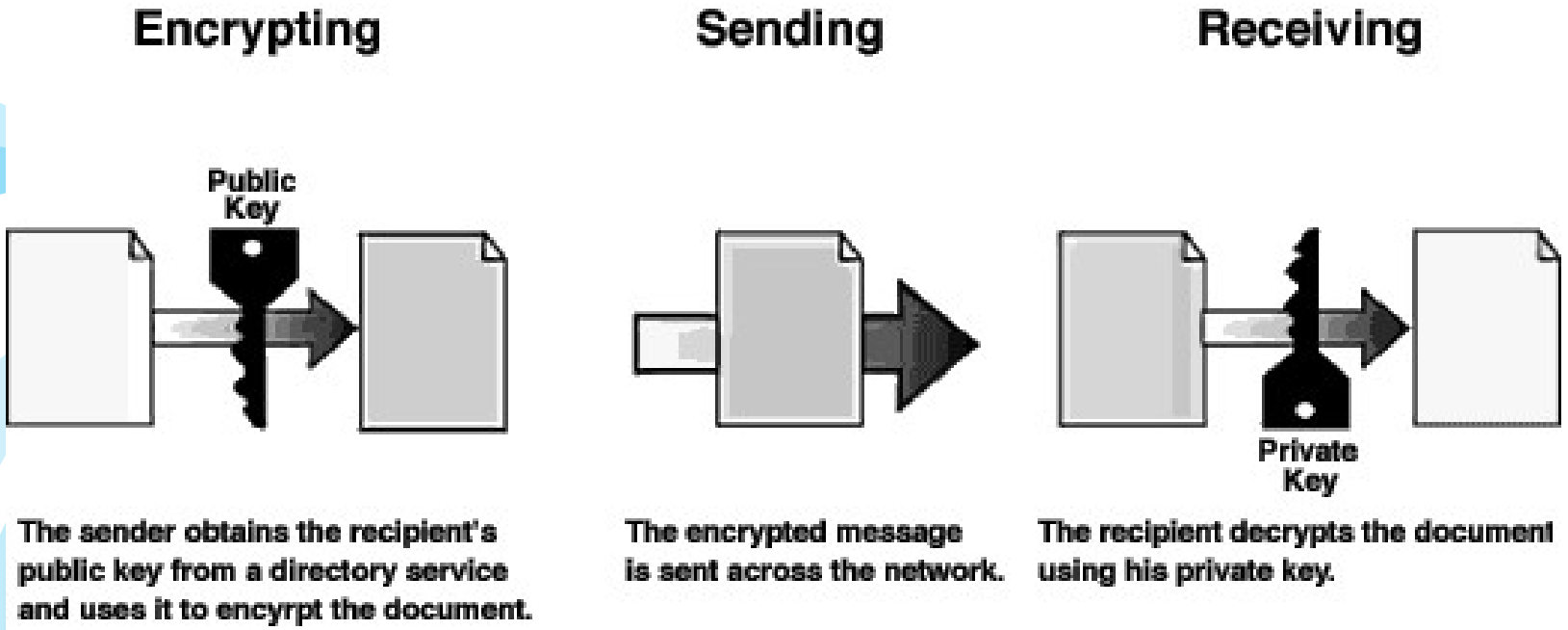
Implementation

- Ability to add new attributes [2]
- Continuity of signature capability [2]
- Counter signatures [2]
- Independent Verifiability [2]
- Interoperability [2]
- Multiple signatures [2]
- Transportability [2]

HIPAA and Encryption

- Regardless of the ambiguity in the Security Rule on this issue, given the risks:
  - Clearly it is in the best interest to assume the stronger posture
  - Apply encryption techniques on any data traffic that flows over the Internet

Basic Encryption with No Signature



Signatures and Access

- Many hospitals allow physicians access to all patient records
  - Not just the patients they're treating, to be sure they have information needed in an emergency
- Concerns about inconvenience of more stringent authentication systems have led to reliance on more convenient (and less secure) log-in IDs and passwords

Signatures and Access

- Many organizations don't maintain audit logs of accesses to clinical data
  - Others have audit logs but haven't developed tools or procedures for systematically reviewing those logs for patterns of abuse
- Vendors haven't put advanced security features on their systems because healthcare organizations haven't demanded them
  - Vendors have focused development efforts in functional areas

Public Key Infrastructure

- While often confused with digital signatures, PKI provides several types of encryption binding which can also be extended to combine the use of digitally signing documents with the process of security encrypting them
- PKI is a complete technology infrastructure that enables users of an unsecured public network (such as the Internet) to securely and privately exchange data

Public Key Infrastructure

- PKI is accomplished through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority
- A digital certificate is the complete package of a public key, a unique name, and the assurance by the certificate authority that the public key belongs to an individual

HIPAA Digital Signature and PKI at Work

- PKI requires use of public-key technology
- In a public-key system, there are two keys: one that is public and can be disclosed and one that is private and must be known only to the individual and the certificate authority
- A certificate authority (a trusted third party) issues public-private key pairs, authenticates the identity of the individual to whom the keys are assigned, and binds a public key by digitally signing a document that contains identifying information

HIPAA Digital Signature and PKI at Work

- A digital signature is formed by applying a mathematical function to the electronic document. This results in a unique bit string, referred to as a "message digest"
- Then, the digest is encrypted using the originator's private key
- The resulting bit stream is appended to the electronic document, and the document is transmitted over a communications network

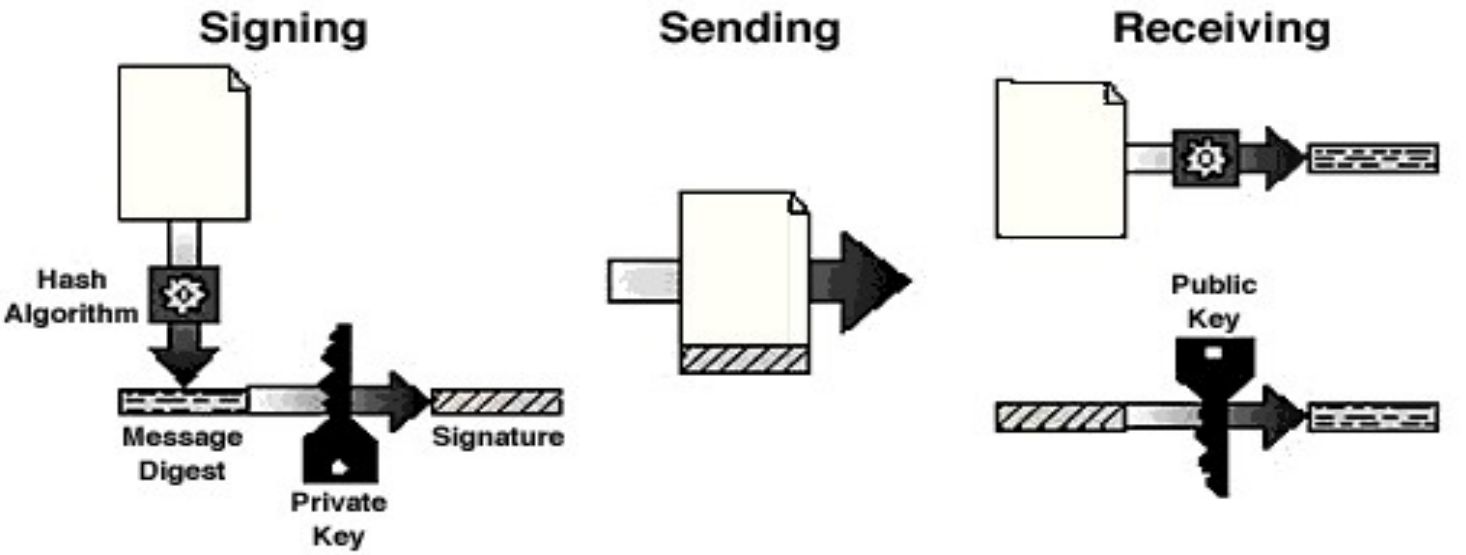
HIPAA Digital Signature and PKI at Work

- The person receiving the document decrypts the message digest with the originator's public key
- Applies the same message hash function to the document, and then compares the resulting digest with the transmitted version
- If they are the same, the recipient is assured that the message has not been altered in transmission and the identity of the signer is proven

HIPAA Digital Signature and PKI at Work

- Since only the person who signed the original document can hold the private key used to digitally sign the document, the critical feature of non-repudiation is also enforced
  - The originator cannot deny signing a document that can be successfully decrypted with his public key

Encryption and Digital Signing



When the sender signs the document it is passed through a hashing algorithm to create a message digest and encrypted using the sender's private key

The signed message is sent across the network.

When the recipient verifies the sender's signature, the same hashing algorithm is used to create a message digest and the signature is decrypted using the sender's public key. If the two are identical, the signature is valid and the document has not changed since it was signed.

PKI Caution

- Many technological, legal, financial, organizational and administrative questions remain to be answered
- Interoperable PKI technology and supporting policies, procedures, and practices will be integral to secure exchange of health information over the Internet

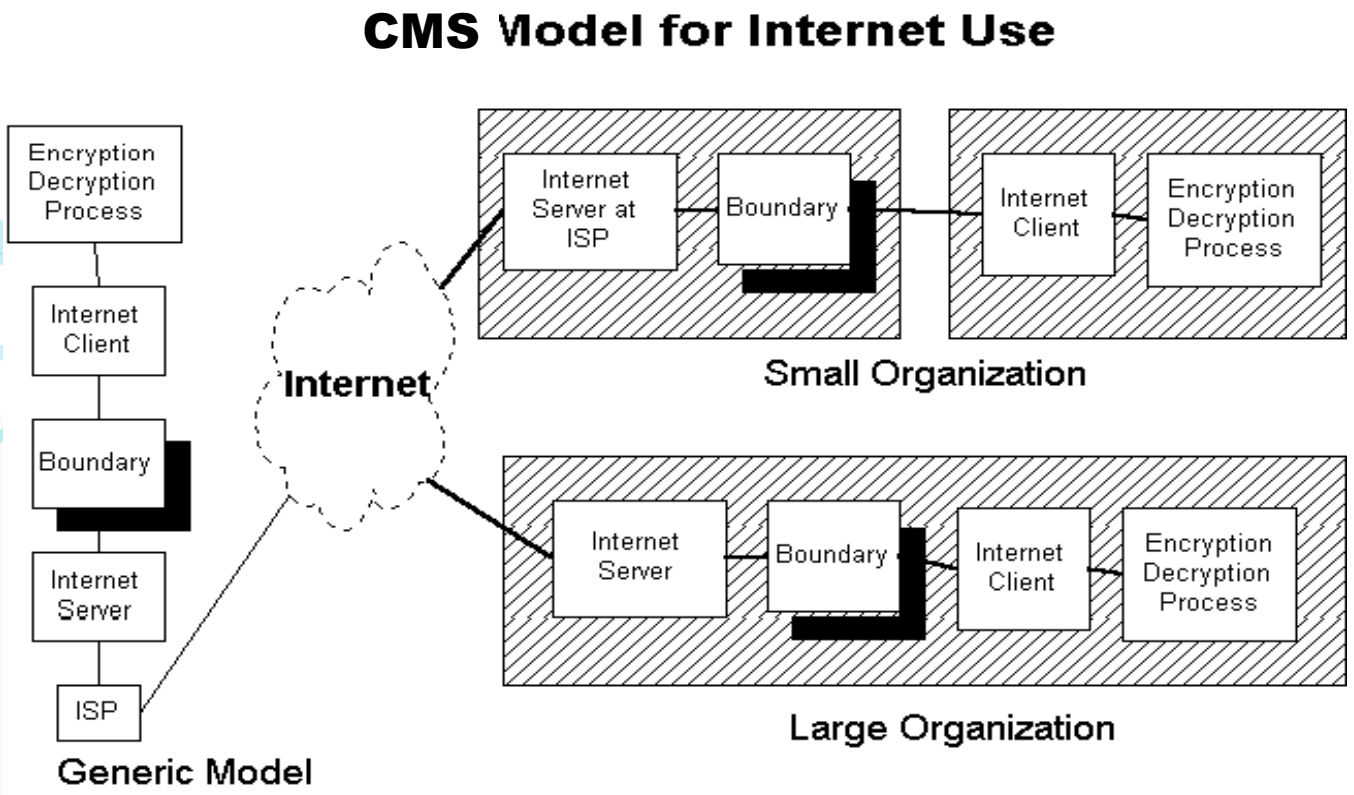
PKI Healthcare Issues

- A public-key management infrastructure, an essential requirement for digital signatures, is not yet available
- Although preliminary efforts are underway to establish such infrastructures in the banking and Internet commerce communities, to date, similar efforts have not been seen in the healthcare industry

PKI Healthcare Issues

- An effective public-key management infrastructure would be required to certify
  - Provider organizations
  - Physicians
  - Nurses
  - Other allied health personnel, and patients themselves
- Significant challenges remain to develop a key management capability that is usable for healthcare

CMS (HCFA) Non-PKI and Signature Model



Connecting Healthcare®
Engaging Patients™
Communicate Educate Motivate™

Have Questions?

Visit our Website,
send us an email,
or give us a call!

(904) 435-3456
(904) 435-3457
Questions@
ConnectingHealthcare.com