

Electronic Signature



```
1 1 0 1 1 1 0 1 0 1 0 1  
0 1 1 1 1 0 1 0 1 0 1 0  
1 0 0 1 0 1 1 0 1 0 0 1  
0 1 0 1 0 0 1 1 0 1 0 1  
1 1 0 1 0 1 0 0 0 1 0 1  
0 1 0 1 0 1 0 1 0 1 0 1
```

Implementing Electronic Signature

Ann Geyer
Bill Pankey

Tunitas Group
209-754-9130
ageyer@tunitas.com
bpankey@tunitas.com



Electronic Signature

✍ Term defined by law

- Federal E-SIGN Legislation*
- State versions as allowed by E-SIGN*

✍ Implemented thru a variety of technologies

- ‘Signature by computer code entry’*
- ‘Signature captured electronically’ or ‘Digitized signature’*
- ‘Signature dynamics’*
- ‘Biometric signature’*
- ‘Digital signatures’*

Expedient Implementations Often Overlook Important Issues

- ✍ **Recognize special requirements for different signature purposes**
 - Patient Consent
 - Authority for medication and other orders
 - Data authenticity (medical records)
 - Execution of business agreements

- ✍ **Poorly designed eSignature application will have consequences**
 - Compliance (state law, criminal statute, payer COP)
 - Liability defense
 - Patient & Practitioner satisfaction
 - Enforceability of business agreements

- ✍ **Stakes are high**
 - Major source of Type I JCAHO advisory
 - Potential for Significant Penalties
 - Litigation
 - Reputation / Physician goodwill

Magee-Womens Hospital (Case on Point)

- ✍ **300 bed tertiary care facility affiliated with the University of Pittsburg Medical Center**
- ✍ **Implemented electronic signature for its lab systems**
 - *Routinely affixed pathologists' 'electronic signature' to reports*
- ✍ **Lawsuit initiated by several pathologists**
 - *To repudiate the signature placed on negative pap smears*
 - *Pathologists claimed they never reviewed results purportedly certified by them*
 - *Allegations of fraud and improper diagnosis*
- ✍ **Class action suit by patients**
 - *Seek retesting of all women who had pap smears reviewed by Magee-Womens between 1995 and 2001*
- ✍ **Investigation launched by CMS**
 - *Pathologist seeking relief under 'whistleblower' statues*

What Magee Womens is now learning

✍ The critical role of policy

- *Magee-Womens P&P did not ensure clear distinction between*
 - *Attestation of physicians, and*
 - *Technician action that merely implied oversight by physician*
- *Review and certification of electronic signature implementations*

✍ Practitioner sensitivity to institutional use of their signature

- *Magee-Womens discounted the interest of their practitioners*
 - *Liability and reputation issues*

✍ Wide ranging ramifications of faulty eSignature use

- *Authenticity of all, not just the disputed, records now being questioned*
- *Additional scrutiny by state & payers sure to follow*
- *Damage to reputation from very public dispute*

Not all publicity is good ...

CNN.com - Suit claims hospital's Pap tests falsely certified - Dec. 19, 2003 - Microsoft Internet Explorer

Address: <http://www.cnn.com/2003/HEALTH/12/19/pap.tests.ap/>

CNN.com MEMBER SERVICES MAKE CNN.com YOUR HOME PAGE

SEARCH The Web CNN.com Search Enhanced by: Google

Home Page
World
U.S.
Weather
Business at cnnmoney
Sports at 5l.com
Politics
Law
Technology
Science & Space
Health
Entertainment
Travel
Education
Special Reports

HEALTH

Suit claims hospital's Pap tests falsely certified

Friday, December 19, 2003 Posted: 10:51 AM EST (1551 GMT)

Story Tools [SAVE THIS](#) [EMAIL THIS](#) [PRINT THIS](#) [MOST POPULAR](#)

PITTSBURGH, Pennsylvania (AP) -- The University of Pittsburgh Medical Center certified thousands of Pap tests when they were never reviewed by physicians, putting an unknown number of women at risk of diseases that may have gone undetected, two lawsuits allege.

The suits filed Wednesday and Thursday allege the medical center's Magee-Womens Hospital routinely misled patients into thinking their tests were examined by doctors by putting doctors' electronic signatures on test results.

The hospital believed it could get more

HEALTH LIBRARY
In association with [MayoClinic.com](#)
• [Health Library](#)

YOUR E-MAIL ALERTS

Search Jobs MORE OPTIONS
Enter Keywords
Enter City ALL
[careerbuilder.com](#) SEARCH

CALL OR VISIT YOUR DOCTOR AS SOON AS SYMPTOMS APPEAR!
[CLICK HERE TO LEARN MORE.](#)

Next time you travel, stay at a CNN Partner Hotel.

SERVICES
Video
E-mail Services
CNNtoGO
Contact Us
SEARCH
Web CNN.com

Internet

Session Objectives

- ✍ ***Information to guide eSignature planning***
 - *Anticipate the business, legal and technology issues*

- ✍ ***Instill greater confidence in the appropriateness of electronic signature***
 - *Understand the changing legal and regulatory environment*

- ✍ ***Provide a framework for evaluating esig technology options***
 - *Advice for ensuring an appropriate level of control*
 - *Methods for maximizing return on investment*

Agenda

- ✍ ***Why implement electronic signature?***
- ✍ ***Where can electronic signatures be used?***
 - *Regulatory and legal analysis*
- ✍ ***How can electronic signatures best be created and maintained?***
 - *Signature related risks and mitigation*
 - *Precursors to implementation*
 - *Electronic signature technology*
 - *Speculating about the HIPAA Esig Rule*
- ✍ ***Examples and Case Studies***
- ✍ ***Implementation Steps***

Agenda

- ✍ ***Why implement electronic signature?***
- ✍ ***Where can electronic signatures be used?***
 - *Regulatory and legal analysis*
- ✍ ***How can electronic signatures best be created and maintained?***
 - *Signature related risks and mitigation*
 - *Precursors to implementation*
 - *Electronic signature technology*
 - *Speculating about the HIPAA Esig Rule*
- ✍ ***Examples and Case Studies***
- ✍ ***Implementation Steps***

Why Implement Electronic Signature?

✍ Healthcare Esig Value Propositions

- Improved compliance with state & federal regulation
 - Automating processes that require signature*
 - Eg. CPOE applications**
- More efficient workflow*
- Greater transaction completion*
- Reduced document cost*

Compliance

- ✍ ***Many signature acts are mandated by state or federal healthcare regulation, such as:***
 - *State mandates*
 - *Medical practice acts*
 - *Health and Safety Code, especially as pertains hospital licensing*
 - *Insurance Code*
 - *DEA rules for prescription of controlled substances*
 - *FDA rules for trials, suppliers, and equipment*
 - *CMS Patient Health Record rules (for Medicare reimbursement)*
- ✍ ***Multiple methods for assessing compliance***
 - *JCAHO*
 - *Whistleblowers and complaints*
 - *Regulator audit*

Why Compliance is Challenging

- ✍ ***Signers often not under the control of the regulated organization***
 - *Practitioners and consumers*
- ✍ ***Signer inconvenience or transparent benefits***
 - *Practitioners*
 - *Many consider the requirements as inconveniences with little or no impact on care or with minimal financial benefit*
 - *Full compliance means chasing signatures -- physically bringing the paper record to the signer for signature*
 - *Multiple FTE dedicated to single task of signature acquisition*
 - *Coercive approaches generally ineffective except perhaps for residents*
 - *Consumers*
 - *Don't see the benefit of signing acknowledgements and agents don't want to retard the purchase process*

Esig Compliance Benefits

✍ Esig provides more opportunities for compliance

- Allows practitioners & consumers to sign at time and location of their convenience*
- Reduces the signer's burden for document return -- reduces dependency on fax, mail or courier*

✍ Currently, advantage may be limited

- To a subset of practitioners, members, other signer types; or a subset of documents, forms, or transactions*
- Subset will expand in keeping with the growth of electronic business processes, Internet applications and similar trends*
- Some HCO already successful in eliminating handwritten signature options for certain healthcare activities*
 - Typically has required a 'paperless' mandate*

Signature and Workflow

✍ Signature acquisition is a single aspect of some business process

- Often gates future action, i.e. can't proceed until signature is acquired*
 - For example, where the signature is an authorization or signoff on discharge summary*

✍ Non-electronic workflow sequences

- Resist electronic management controls: reporting, routing . . .*
 - Where is the paper vs
Where is the electronic record?*
- Are fragile due to potential for lost, misdirected or misfiled records*
- Include some additional steps to support conversion to and from paper formats*

Esig Workflow Benefits

✍ Process efficiencies

- Complete work faster*
- Eliminate or reduce duplicate signature procedures*
- Displace signature acquisition costs*
- Enable integrated record keeping*
- Record, transmit and track signed documents easier*
- Provide greater user and staff convenience*

Online eHealth Transactions

✍ Higher Transaction Completion Rates

- *Transactions initiated online often have lower completion rates whenever the process must stop for an ‘out of band’ activity*
 - *Consumer loses interest, fails to complete activity*
 - *Necessary information fails to arrive*
- *Esig allows online, uninterrupted transaction completion*
 - *Reduces failure rate*
 - *Reduces completion time*
 - *Reduces management cost*

✍ Caveat

- *Special rules apply to electronic signature for some consumer transactions, for example*
 - *Dis-enrollment from health plan*
 - *Pre-agreement to conduct some transactions electronically is required*

Reduced Document Cost

- ✍ Electronic signature may obviate last requirements for paper***
- ✍ Displace costs associated retention of physical paper records***
 - Paper*
 - Printing, reproduction, shipping*
 - Filing*

Esig Overview ~ Basic Questions

- ✍ **Why implement electronic signature?***
- ✍ **Where can electronic signatures be used?***
 - **Regulatory and legal analysis***
- ✍ **How can electronic signatures best be created and maintained?***
 - **Signature related risks and mitigation***
 - **Precursors to implementation***
 - **Electronic signature technology***
 - **Speculating about the HIPAA Esig Rule***
- ✍ **Examples and Case Studies***
- ✍ **Implementation Steps***

Electronic Signature Is a Means of Obtaining Signature – Nothing New Here

- ✍ ***Electronic signature should have presumption of validity, unless precluded by statute***

- ✍ ***The traditional signature concept includes:***
 - *“any mark ... made on a document and intended to serve as an indication of the party's execution or authentication of the document and intent to be bound by it” ~ Martindale-Hubbell Law Directory*

 - *The signature concept easily supports the idea that electronic “marks” can be signatures*

Caveat

- ✍ **... Many sources of bias against electronic signature**
 - *‘Wet signature’ laws and regulations require handwritten signatures and retention of original paper records*
 - *E.g., DEA rules require examination of ‘original signature’ on prescription before dispensing narcotic*
 - *Blue ink regulations over form and method of signature*
 - *State prescription laws*
 - *State medical records regulation*
 - *Payer rules*
 - *Medicare “Certifications of Medical Necessity”*
 - *Statutes of fraud that require ‘tangible evidence’ of contract*
 - *Limit enforceability to written contracts*
 - *Especially as pertains to real estate contracts*
 - *Wills and testamentary trusts excluded from E-SIGN legislation*

E-SIGN

- ✍ ***Electronic Signatures in Global and National Commerce Act (ESIGN) -- US Public Law 106-229***
 - *“An electronic signature is any electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record”*

- ✍ ***E-SIGN preempts contrary state law or federal regulation***
 - *“A signature ... may not be denied legal effect, validity or enforceability solely because it is in electronic form”*

E-SIGN Mandate to States & Federal Regulators

- ✍ Regulators required to rewrite rules to allow for electronic signature and electronic record retention***

- ✍ Agencies may set 'performance standards' for covered transactions to ensure***
 - Availability and integrity of retained transaction records*
 - Authenticity of signature*

- ✍ Rule-making Restrictions***
 - Requires substantial justification to proceed*
 - Must be essentially equivalent to rules applying to non-electronic transactions and may not re-impose any paper requirement*
 - Must be reasonable in implementation cost*
 - Must be technology neutral*

E-SIGN Preemption Mandate

- ✍ ***Agencies may require specific technology, but only if the use***
 - *Serves a substantial government objective*
 - *Is substantially related to that objective*
 - *Even then, may not require specific hardware or software*

- ✍ ***E-SIGN requires states / agencies to promulgate revised rules by June 1, 2001***
 - *Few agencies have explicitly complied*

- ✍ ***OMB Guidance on Implementing E-SIGN, in absence of a rule revision***
 - *Covered parties are free to retain records in electronic form of their choosing*
 - *Know your regulator!*

Removing Vestiges of Wet Signature Laws

- ✍ **Most states have adopted “Uniform Electronic Transactions Act” (UETA)**
 - Others have esig law predating UETA with specific provisions regarding digital signature (eg WA, IL, UT)

- ✍ **UETA implements E-SIGN at the state level**
 - Generally rescinds regulation requiring handwritten signatures
 - Gives autonomy to the parties of a transaction to determine method of implementing electronic signature
 - Provides guidance (to courts) for resolution of esig disputes
 - e.g. establishes responsibilities to mitigate errors

- ✍ **Most rules have not been rewritten, but should be interpreted in context of UETA or non-preempted portions of state’s Esig law**

- ✍ **Again important to know your regulator!**
 - Agency may have specified a ‘performance’ standard
 - Agency may have “idiosyncratic” preemption analysis
 - e.g. DEA position that prescription of narcotics is not “in or affecting interstate commerce”

Federal Paperwork Elimination Mandate

- ✍ **E-SIGN addresses rules for transactions to which a state or federal agency is not a party***

- ✍ **Government Paperwork Elimination Act (GPEA) Title VII of Public Law 105-277 affects transactions to which a federal agency is a party***
 - Requires that agencies must support electronic submission of any form it now receives >50,000 filings per year*
 - e.g. Medicare Certificates of Medical Necessity*
 - Forms for portable oxygen, dialysis patients that require physician's blue ink signature*
 - Agencies are required to implement multiple alternate methods for electronic submission*
 - Compliance date, October 2003*
 - Medicare currently not compliant*
 - Agency cannot mandate electronic submission*
 - Conflict CMS requirement for electronic transactions*

Summary ...

- ✍ **Generally can use electronic signatures anywhere**
- ✍ **Statutes requiring 'handwritten' signatures are explicitly satisfied by Esig, but**
 - *Regulators & legislators are slow to update rules; some antiquated rules still remain -- DEA & CMS*
 - *States may have own esig law whose objectives are generally consistent with E-SIGN*
- ✍ **Future Esig regulations must be 'technology neutral'**
 - *Can only require specific technology if doing so serves a compelling government interest. Some state regulation at risk*
- ✍ **Consumer applications require special design considerations**
 - *Consumer protection concerns*

Esig Overview ~ Basic Questions

- ✍ **Why electronic signature?***
- ✍ **Where can electronic signatures be used?***
 - Regulatory and legal analysis*
- ✍ **How electronic signatures can best be created and maintained?***
 - Signature related risks and mitigation*
 - Precursors to Implementation*
 - Technology of electronic signature*
 - Speculating about HIPAA*
- ✍ **Case Studies***
- ✍ **Implementation Steps***

Technology Requirements

✍ Functional requirements derived from:

- Esig definition*
 - Identify signer*
 - Recognize and record signer's intent*
- Applicable regulatory mandates*
 - State medical records, prescription law*

✍ Non-functional requirements are derived from:

- The need to anticipate any future dispute over signature validity*
- Assumption that signature will never be disputed, implies that there is no need for signature*
- Signature should be part of security apparatus designed to cost effectively minimize risk*

Two Significant Risks

	Signature Intent	No signature Intent
Successful assertion	OK	RISK (false assertion)
Successful repudiation	RISK (false repudiation)	OK (quality control measure)

- ✎ **Effective esig implementation will minimize the consequences associated with:**
 - False Assertion
 - Attributes an electronic signature where there was not a valid one
 - False Repudiation
 - Signer successfully denies responsibility for his / her signature act
 - Effort to prevent any repudiation may be misdirected

- ✎ **Analysis of failure conditions provides basis for implementation decisions**
 - Consequence of signature only recognizable where authenticity is disputed

Scenarios ~ False Assertion

- ✍ ***Hospital organization improperly attributes an electronic medication order to a named practitioner***
 - *Patient safety issues*
 - *Practitioner dissatisfaction. Doc knows that he did not sign!*

- ✍ ***Health plan accepts forged signature on certificate of medical necessity for durable medical equipment***
 - *Fraud related financial loss that is borne but not recognized*
 - *Sarbanes-Oxley concern for publicly traded health insurer*

- ✍ ***Hospital records in medical record unsigned clinical notes ... as if they were signed***
 - *Potential prejudicial impact to patient.... Especially when notes not intended to be disclosed as part of 'legal' record*

Risk - False Assertion

✍ Usually due to failure of operational controls

- Where operational control over the Esig mechanism fails
 - Prevent impersonation of the purported signer, or*
 - Prevent record modification after signing**
- Also, poor UI design may mistake signer intent*

✍ Consequences

- Are not immediately apparent to party relying on signature*
- May be limited to the impacted transaction
 - Can the transaction be revoked? at what cost?*
 - If not revocable, what is the recovery cost?**

✍ Expected loss calculation

- $L = \min[c(R), c(T)] * [p(I) + p(M) - p(I)*p(M)]$*
- where $c(R)$ = cost of recovery, $c(T)$ = value of transaction; $p(I)$ = likelihood of impersonation; $p(M)$ = likelihood of modification*

Scenarios ~ False Repudiation

- ✍ ***Clinician successfully denies responsibility for an order / medication dispensed under the clinician's authority***
 - *Creates inappropriate distrust in EOE and MARS*
 - *New liability exposure*

- ✍ ***Patient successfully denies authorizing PHI disclosure***
 - *Privacy complaint and OCR sanction*

- ✍ ***Employee / affiliated practitioner denies formal acceptance of 'user agreement' / COP***
 - *Reduced ability to apply sanctions / enforce policy*

Risk - False Repudiation

*✍ **Usually due to a design failure***

- Where the esig mechanism does collect sufficient evidence to successfully dispute the repudiation*

*✍ **Consequences***

- Extend beyond the disputed transaction
 - Provides precedent for repudiation of other transactions**
- Significant organizational impact if the healthcare organization challenges repudiation of its practitioners*

*✍ **Expected loss calculation***

- $L = (\min((c(Lit) + .2*(c(J)),c(S))) * P(D)$*
- where: $c(Lit)$ = litigation cost, $c(J)$ = judgement requested; $c(S)$ = anticipated settlement; $p(D)$ - probability of dispute*

Esig Overview ~ Basic Questions

- ✍ **Why electronic signature?***
- ✍ **Where can electronic signatures be used?***
 - Regulatory and legal analysis*
- ✍ **How electronic signatures can best be created and maintained?***
 - Signature related risks and mitigation*
 - Precursors to implementation*
 - Technology of electronic signature*
 - Speculating about HIPAA*
- ✍ **Case Studies***
- ✍ **Implementation Steps***

Esig is not just technology

✍ Business, Legal, and User Contexts are Critical

- *Do persons recognize that the particular esig action will have legal consequence?*
 - *Mouse clicks don't naturally have the 'gravitas' of handwritten signature*
- *Demonstration of person's intent is critical to the assertion of a particular electronic signature*
 - *When user clicked 'ok', did he really intend to wipe his hard drive?*

✍ Two cases to consider:

- *Workforce and affiliated practitioners, contractors, etc*
 - *Persons who sign the organization's documents on a regular and routine basis*
- *Consumers*
 - *Infrequent users of esig at best*

Electronic Signature Policy ...

Workforce

- ✍ ***Policy binds use of esig technology to business agreements and standard practices of organization***
 - *Establishes esig 'business rules'*
 - *Binding upon workforce*
 - *Fixes responsibility for operational control over esig mechanism, retained records, etc*
 - *Should be a formal policy document*

- ✍ ***In medical context, policy should include procedures to collect practitioners' explicit acceptance of signature mechanism with an intent to be bound by its use***
 - *Regulatory requirement for some applications*
 - *State medical records law*
 - *Per FDA CFR 21 Part 11, implementer must assert intention to treat Esig mechanism as equivalent to legally binding handwritten signature*
 - *Don't forget the need to update Medical Staff ByLaws*

Some Issues addressed by Policy

✍ Limits on electronic signature use

- *What documents may be signed electronically?*
 - *Who makes that determination?*
- *Who may sign those documents?*
 - *Is there an approval process?*
- *What are the [strength of] assurance requirements?*
 - *Are there any environmental constraints? (e.g. can orders be signed ‘over the web’?)*

✍ Sanction

- *What sanctions apply when users do not responsibly use / protect signature mechanisms assigned to them*

✍ Exception handling

- *What happens when electronic signature mechanism not available? Revert to paper? Delay signature?*

✍ What is status of unsigned records / files?

- *Viewable? By whom?*
- *Modifiable by signer?*

✍ Do multiple signers have additional responsibility?

Electronic Signature Policy ~ Consumers

- ✍ ***Establish approval process for esig application***
 - *Who determines that application provides all consumer protections required by E-SIGN and applicable state law?*
 - *E.g. preserve ability for timely revocation;*
 - *E.g. provision for consumer to have a paper copy of signed record.*

- ✍ ***Consumer applications may involve challenging user authentication issues, need special concern:***
 - *Risk parameters should be established as a matter of policy*
 - *How much risk can particular esig applications bear (more later)*

RFC 3125 – ‘Electronic Signature Policy’

- ✍ ***Useful where party relying upon signature is different from party maintaining electronic signature application***
 - *E.g., hospital collecting physician signature on health plan required certification of medical necessity*
 - *Health plan may or may not accept hospital’s esig scheme*
- ✍ ***Policy framework for negotiating technology requirements***
 - *Basis for automated verification of electronic signatures*
- ✍ ***Policy elements include:***
 - *Limitations on the types of transactions for which esig will be used*
 - *Rules relating to trust infrastructure and required esig attributes*
- ✍ ***RFC 3125 appropriate for digital signatures but concepts more generally applicable***

Understanding Dispute Resolution

Can Bridge Policy & Technology Choices

✍ UETA provides guidance for the resolution of esig disputes

- Uniform Electronic Transaction Act Model codes*
- Allows trading partners to choose method of implementing Esig*

✍ Esig dispute resolution

- Generally requires showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.*
- Risk analysis helps calibrate the design and operation of esig system*
 - Value of transaction, costs or recovery, litigation, etc*
 - Provide cost basis for esig controls*

✍ Dispute resolution framework should be addressed in esig policy document. Technology provides evidence for assertion

Esig Overview ~ Basic Questions

- ✍ **Why electronic signature?***
- ✍ **Where can electronic signatures be used?***
 - Regulatory and legal analysis*
- ✍ **How electronic signatures can best be created and maintained?***
 - Signature related risks and mitigation*
 - Precursors to Implementation*
 - Technology of electronic signature*
 - Speculating about HIPAA*
- ✍ **Case Studies***
- ✍ **Implementation Steps***

Caveat ... Product Limitations

- ✍ ***Many EMR products lack any significant abstraction of esig components***
 - *Implementation flexibility limited to configuration options of vendor products*
 - *Typically such products only support minimum esig practices as typified in JACHO IM standards / hospital licensing rules*
 - *Implementer task focused primarily on establishing policy and supporting administrative infrastructure*

- ✍ ***Choice of esig technology is most meaningful outside context of vendor supplied EMR system***

Esig Application Components

✍ Signer identification and authentication

- Authentication can occur at any time, before or after signature act*
- Signer authentication typically implies user registration and/or user database*

✍ Signature capture

- Record the intention of the signer*
 - Examples: User's key stroke response to windows prompt; biometric capture; sound recording; digital signature computation*
- Intention may be easily disputed with ephemeral electronic UI, need support of a business & legal infrastructure*
 - Validation with signer community*

✍ Record retention

- Must be in a form that ensures accurate reproduction*

Important Esig Properties

- ✍ **Not all properties satisfied by every technology or implementation**
 - **Uniqueness** ~ signatures of unique signers are distinguishable
 - **Independent verifiability** ~ signature verification can be accomplished without the participation of the signer or the system that created the signature
 - **Persistence** ~ signature is available for verification after system changes or extended passage of time
 - **Transportability** ~ signature can be communicated across communications network
 - **Non-Repudiation** ~ a measure of the difficulty a signer will have in denying responsibility for a signature. Typically understood to mean that the signer has the burden of proof when denying signature.

Properties affect importance of the non-functional aspects

- ✍ ***Is any confidential information required to construct signature unique to signer?***
 - *If not then non-repudiation is unlikely*

- ✍ ***Is confidential information required to verify signature?***
 - *Does the signature verifier need knowledge of confidential information? Such as PIN, biometric template or other*
 - *Determines whether independently verifiable; affects non-repudiation*

- ✍ ***How is the signature represented as 'data'?***
 - *Is the representation independent of the application that created the signature*
 - *Determines whether the signature is transportable*

- ✍ ***How is the integrity of the signature maintained?***
 - *Does integrity depend on the continuous enforcement of application, system and business controls?*
 - *Determines the long term persistence of signature, affects non-repudiation*

Signature properties and use

- ✍ ***Esig properties are important for different record purposes***
 - ***Compliance: uniqueness; non-reputability (proforma)***
 - *Requirements typically set by regulation; typically requires some signer attestation of responsibility*
 - ***Reimbursement: independent verifiability; transportability***
 - *There has to be something to send payer; payer would not normally interact with the provider system that collected the signature*
 - ***Liability defense: persistence, non-reputability***
 - *Liability disputes may occur long after signature act. Signature disputes will be resolved by challenging the reliability of the application creating the signature. Burden of proof typically will fall onto the application owner.*
 - ***Business Contracts: uniqueness, non-reputability***

Some Esig Technologies

- ✍ ***Simple Sign***
- ✍ ***Computer Code Entry***
- ✍ ***Digitized Signature***
- ✍ ***Digital Signature***

Simple Sign

✍ E-SIGN recognizes very simple schemes for esig

- Pressing button labeled ‘ok’ or ‘sign’*
- Some basis to determine ‘signer’s identity’*
 - User identity provided by context, such as CURRENT_USER or information on completed form*
 - No explicit requirement for security / authentication infrastructure*

✍ Advantages

- Rapid completion of online transactions, especially with persons for whom there is not an ongoing business relationship*
 - Health plan enrollment where signature is needed to authorize request for medical records*

✍ Disadvantages

- Not particularly useful for general healthcare purposes where signer authentication is required*
 - HIPAA’s ‘appropriate safeguards’*

Issues

✍ **May be easy to repudiate**

- *Impersonation may be easy*
 - *However, signer's identity can be shown by any evidence*
 - *What action is triggered by the executed record?*
 - *Does that action allow subsequent identity corroboration?*
 - *Funds transfer or check?*
 - *Delivery of goods to signer's address?*
- *What 'proves' intent of signer?*
 - *What is potential for misinterpreting the UI?*
Especially when rendered by different browsers,
 - *e.g. 'type size' issues.*
 - *Must consider relevant 'consumer protection' protections*
including ability to retain record / timely signature revocation

✍ **Should weigh benefit of transaction completion against easy repudiation**

Signature by Computer Code Entry

✍ Typical medical records practice

- Supported in major patient record / EOE systems*
- Explicitly endorsed in existing hospital licensing reg. of many states; JCAHO IM standards*

✍ Three components to method

- Person's attestation of 'code' ownership, promise of exclusive use, and acceptance of responsibility for any use*
- Person's entry of code to indicate signature intent*
- System of technical security controls to prevent record modification subsequent to 'signing'*

✍ Advantages

- Simple to implement in 'secure' record systems*
- Easily implemented over network*

Issues

- ✍ ***There is no explicit representation of the signature***
 - *If the record contains the entry, then it must have been signed because that is the way the system is built*
 - *Signature is only implicit in the execution of the system's business rules*

- ✍ ***Controls to ensure record or signature integrity are crucial to 'non-reputability'***
 - *Issuance and management of computer codes*
 - *Record locking*
 - *Splitting of administrator roles and oversight*

- ✍ ***Practitioner usability paramount***
 - *Scheme be generalized to include alternate user action / authentication*
 - *Thumbprint; SecureID;*
 - *Invoking CCOW 'authentication_action_agent'*
 - *Beware use of shared (with staff) access codes*

Use

✍ Compliance

- *By definition, the scheme provides the internal controls currently favored by regulators and JCAHO*

✍ Reimbursement

- *Scheme does not provide a signature representation to transmit to payer. Acceptance of records as authentic depends on payer's goodwill and trust in 'signature on file' schemes*

✍ Liability Defense

- *Signature easily repudiated following the plausibility of a failure of any control.*

✍ Contract

- *Accompanying attestation provides explicit basis for UETA required 'agreement to be bound'*

Digitized Signature

- ✍ ***The handwritten signature is captured on an electronic key pad -- first derivative of a 'wet signature'***
 - *Pad creates digitized' image*
 - *Advanced technology may capture signature dynamics*
 - *Measure supposedly biometric invariants of handwriting including speed, acceleration, sequential stroke patterns*
 - *May provide some additional level of signer authentication*
 - *Attach to electronic record*
 - *Intuitive use of familiar practice*
- ✍ ***Require specialized hardware to capture handwriting which limits deployment***
 - *Some support with PDA and Tablet PC*

Issues

- ✍ **How is the signature bound to the signed record?**
 - *Require additional controls to ensure that record is not modified subsequent to signature. Typically these are proprietary schemes whose strength is a matter of vendor claim only.*

- ✍ **How easily can signature be repudiated?**
 - *Once captured, little prevents attaching 'digitized signature' to subsequent documents without signer's knowledge or approval*
 - *"I signed a record but not this record"*
 - *What demonstrates 'original use' of signature and not merely reuse of earlier representation?*

- ✍ **Methodology may lack independent verifiability**
 - *Open standards lacking for signature digitization and 'signature dynamics' impeding vendor neutral implementation*
 - *Dependence on proprietary 'verification' server / software*

Use

✍ Compliance

- *Dependent on controls to ensure that digitized signature was created at time of purported signature (original use)*
- *Difficult to treat as ‘signature stamp’ because reuse outside control of signer. (e.g. the case of Magee Williams)*

✍ Reimbursement

- *Scheme does provide a signature representation to transmit to payer.*

✍ Liability Defense

- *Signature easily repudiated following the plausibility of a failure of controls over reuse.*

✍ Contract

- *Supported by ‘common use’ of handwritten signature*

Digital Signature deserves special attention

✍ **Most secure signature technology**

- Cryptographically binds signer's 'signature key' to 'fingerprint' (hash) of the record
 - Digital signature is sensitive to any record modification
 - Virtually no potential for impersonation
 - Persistent and transportable signature representation

✍ **Presumptive validity in some states (under special conditions)**

- e.g, Illinois 'secure electronic signature', UT, WA

✍ **Good standards support for technical interoperability**

- FIPS 186-2, ANSI X9.62, ANSI x9.32, W3C xml-dsig, X12.58
- DICOM Profiling / ASTM e2084 healthcare standard

✍ **Multiple industry recommendations**

- HIPAA Security and Electronic Signature NPRM; HISB Joint SDO Signature Study; DEA Rules for electronic prescriptions

How Digital Signature Works

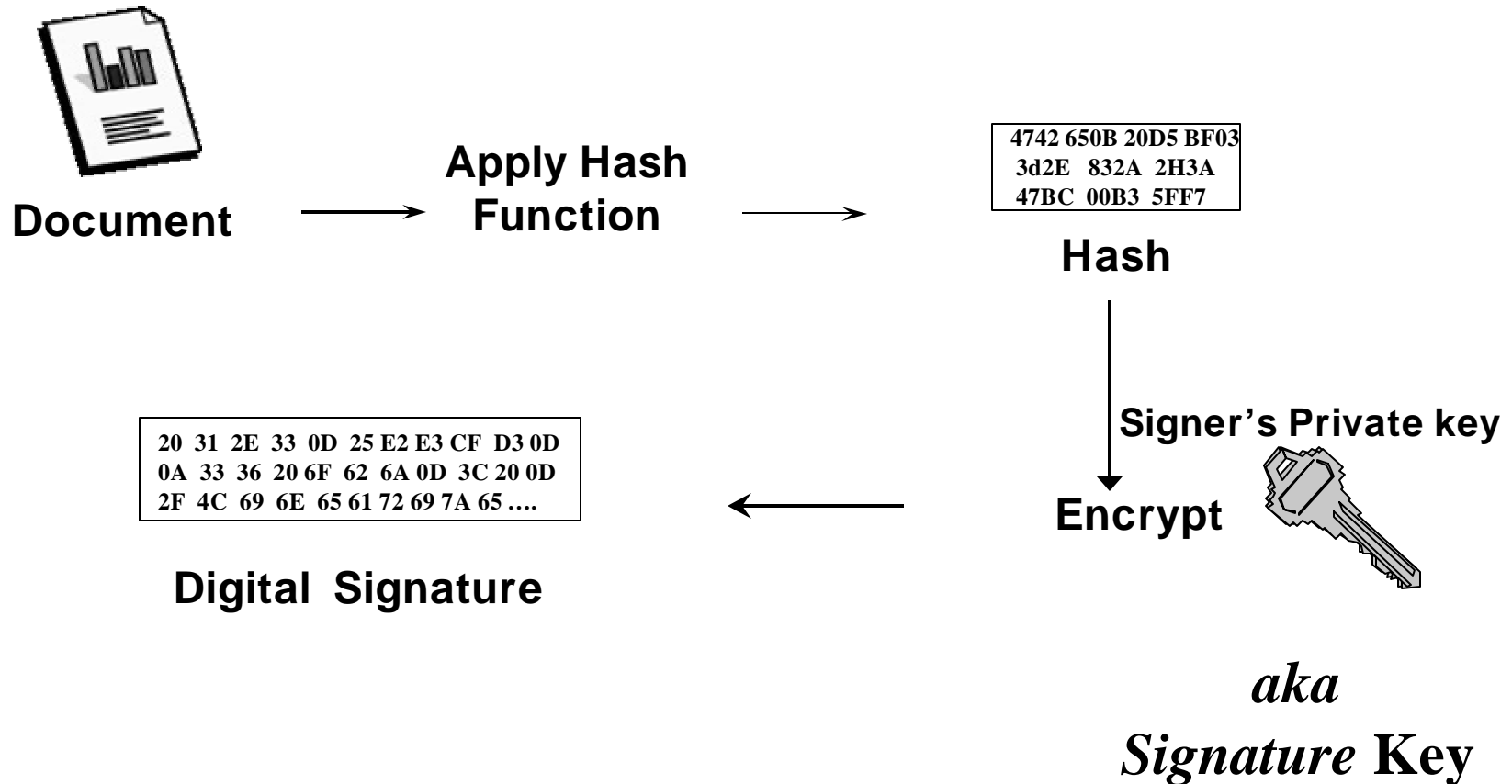
✍ Asymmetric (public key) cryptography involves 2 mathematically related keys

- *‘Public key’ which is the ‘inverse’ of the ‘Private key’*
 - *Public key reverses the operation of the private key / vice versa*
 - *Public key is needed to decrypt what is encrypted by related private key*
- *Fundamental tenet of public key cryptography*
 - *Public key is uniquely determined by private key, but*
 - *Knowledge on ‘public’ key will not compromise secrecy of ‘private’ key*

✍ Public key bound to a named individual thru a public key ‘certificate’

- *PKI provides policy and procedure to assure:*
 - *the identity of the bound individual*
 - *The bound individual possesses associated private key*

Digital Signature Creation



Digital Signature Verification

aka

Verification Key

Signer's Public key

```
20 31 2E 33 0D 25 E2 E3 CF D3 0D
0A 33 36 20 6F 62 6A 0D 3C 20 0D
2F 4C 69 6E 65 61 72 69 7A 65 ....
```



```
4742 650B 20D5 BF03
3d2E 832A 2H3A
47BC 00B3 5FF7
```

**Digital
Signature** →

Decrypt →

Hash

Compare



Document →

**Apply Hash
Function** →

```
4742 650B 20D5 BF03
3d2E 832A 2H3A
47BC 00B3 5FF7
```

Hash

Issues

✍ Private (Signature) key ownership

- Certificates identify key pair ownership*
- Traditional role assigned to PKI*
- Certificates are standardized public documents, but must be “trusted” to be useful*

✍ Private (Signature) Key Protection

- Exposure of private signature key compromises the authenticity of an electronic signature*
- Merely requiring the signer ‘to adequately’ protect the private key may be inadequate*
 - Does the individual understand how to do so?*
 - What is the appropriate level of protection?*
 - Sophisticated technical attacks against private keys stored in software, especially in windows key store*

Issues

✍ Implementation complexity

- *w/o high level toolkit, requires specialized developer skills*
- *Requires some sort of PKI deployment to signers*
 - *PKI requires ongoing management*
 - *Mitigated by new enterprise PKI management models*
 - *AR CoSign Signature Appliance*
 - *Window 2000+*
 - *Certs managed as part of system and network administration*

✍ Performance

- *Digital signatures are computationally complex*
- *Potential unsatisfactory performance on mobile devices*
 - *Speed an issue with busy practitioners*
- *Bandwidth for transmission and storage*
 - *1.5-2k bits per signature at a minimum; more depending on enveloping technology.*

Issues

✍ Sensitive to any change in signed record

- *Storage, communication and display must be ‘bit preserving’*
- *May be too strong for many document types*
 - *‘Lossy’ transmission and storage of high bandwidth documents, e.g. radiological images*
 - *For digital signature, every bit is important*
- *Potential solutions thru use of ‘canonical’ document representation*

✍ Corollary: Lack of abstraction

- *Increased abstraction as electronic health records become distributed*
 - *Model –view –controller design philosophy separating presentation from data*
- *Focus on authenticating data, not a particular presentation of it*
 - *But digital signatures defined over concrete representation of data*

Digital Signature Use

✍ Compliance

- Signature uniqueness guaranteed by uniqueness of signer's private key; attestation from the cert subscriber agreement*

✍ Reimbursement

- Provider institutions can readily transmit signature to payers; payers can readily verify practitioner's signature*

✍ Liability defense

- Properly constructed digital signatures can only be repudiated by admission of signer failure to adequately protect private key*

✍ Contracting

- Certificate subscriber agreement usually includes a declaration of the key holder's intent to be bound by associated digital signatures*

Digital Signature Representations

- ✍ **Standards based procedure to represent or 'envelop' the digital signature**
 - *Envelop contains all information needed by 3rd party to verify signer identity and message authenticity, and to properly determine the signer's intention*

- ✍ **PKCS#7 (Public Key Cryptography Standards)**
 - *Defines format for signature data structure using ASN.1*
 - *PKCS#7 makes use of "Basic Encoding Rules"*

- ✍ **XML-DSIG**
 - *Defines XML template for digital signature representation*

- ✍ **DICOM Digital Signature Profile**

- ✍ **X12.58**
 - *EDI standard for encrypting, signing, and compressing the data within an X12 transaction*

Some Digital Signature Tools

✍ Microsoft

- *VB level developer toolkit, CAPICOM*
 - *Create digital signature with 2 lines of code*
- *Digital signature built into Office 2000 and successors*
 - *Digitally sign any Office document*
 - *Options | Security | Digital Signatures*
 - *Cumbersome for end users, need to develop macro for general use*
 - *Use certificates in IE's key store*

✍ Adobe

- *Digital signature built into Acrobat (full and Reader 6+)*
 - *Creates signature keys as needed (self-sign) or use others with plug-in*
 - *Supports optional specification of signature 'purpose'*

✍ OpenSSL

- *Provides functions for basic certificate and signing operations*

Demonstrations

✍ Microsoft support for digital signature

- Office*
- CAPICOM*

✍ Adobe support for digital signature

Esig Overview ~ Basic Questions

- ✍ **Why electronic signature?***
- ✍ **Where can electronic signatures be used?***
 - Regulatory and legal analysis*
- ✍ **How electronic signatures can best be created and maintained?***
 - Signature related risks and mitigation*
 - Precursors to Implementation*
 - Technology of electronic signature*
 - Speculating about HIPAA*
- ✍ **Case Studies***
- ✍ **Implementation Steps***

HIPAA Electronic Signature Standard

- ✍ **1996 HIPAA Law called for HHS to promulgate standards for transmission and verification of electronic signature related to HIPAA reimbursement transactions**
 - 1998 NPRM proposed that standard should involve digital signatures

- ✍ **Limited use case for esig in reimbursement transaction context**
 - Claims are not signed
 - Attached information typically is signed
 - Industry may be satisfied with ‘signature on file’ approach
 - Signature critical to “Certifications of Medical Necessity”
 - e.g. Medicare DME and dialysis certifications
 - Signature transmission is not included in current HL7/ X12 approach to claim attachments
 - If the use case for the attachment potentially involves verification of a signature, the work group has defined ‘not an attachment’
 - HL7 does not directly support transmission of actual signature, instead only the assertion that a particular person signed document

HIPAA Electronic Signature Standard

- ✍ ***HHS current view is to promulgate only standards that have already been widely adopted by the industry***
 - *Implies that there will be NO HIPAA Esig standard*
 - *Mandate to use an ‘attachment standard’ which apparently will define away any requirement for signature transmission*
 - *‘Must accept’ provisions will prevent plan request / requirement for other info /paper to authenticate electronic signature*
 - *Therefore no opportunity for industry to ‘widely adopt’ standard procedure*

- ✍ ***Are Medicare ‘Certifications of Medical Necessity’ health claim ‘attachments?’***
 - *Include patient info transmitted from provider to payer in support of a claim*
 - *How will Medicare support electronic transmission of electronic signature for Certifications as required to do by “Government Paperwork Elimination Act”?*
 - *Medicare so emphasizes ‘original signature’ that in some cases intermediaries requires ‘blue ink’*

Medicare Certifications of Medical Necessity

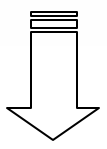
DMERC 484.2 Certification

- submitted by supplier of medical equipment (e.g. portable oxygen) but signed by practitioner
- includes various lab results; clinical evaluation / notes

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
HEALTH CARE FINANCING ADMINISTRATION

FORM APPROVED
OMB NO. 0938-0534
DMERC 484.2

CERTIFICATE OF MEDICAL NECESSITY

OXYGEN		
SECTION A Certification Type/Date: INITIAL ___/___/___ REVISED ___/___/___ RECERTIFICATION ___/___/___		
PATIENT NAME, ADDRESS, TELEPHONE and HIC NUMBER (____) ____ - ____ HICN _____		SUPPLIER NAME, ADDRESS, TELEPHONE and NSC NUMBER (____) ____ - ____ NSC # _____
PLACE OF SERVICE _____ NAME and ADDRESS of FACILITY if applicable (See Reverse)	HCPSC CODE _____ _____	PT DOB ___/___/___; Sex (M/F); HT. (in.); WT. (lbs.)
		
SECTION D Physician Attestation and Signature/Date		
I certify that I am the treating physician identified in Section A of this form. I have received Sections A, B and C of the Certificate of Medical Necessity (including charges for items ordered). Any statement on my letterhead attached hereto, has been reviewed and signed by me. I certify that the medical necessity information in Section B is true, accurate and complete, to the best of my knowledge, and I understand that any falsification, omission, or concealment of material fact in that section may subject me to civil or criminal liability.		
PHYSICIAN'S SIGNATURE _____ DATE ___/___/___ (SIGNATURE AND DATE STAMPS ARE NOT ACCEPTABLE)		

FORM HCFA 484 (11/99)

HCFA 2728

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

FORM APPROVED
OMB NO. 0938-0046

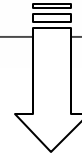
END STAGE RENAL DISEASE MEDICAL EVIDENCE REPORT MEDICARE ENTITLEMENT AND/OR PATIENT REGISTRATION

A. COMPLETE FOR ALL ESRD PATIENTS

1. Name (Last, First, Middle Initial)

2. Health Insurance Claim Number

3. Social Security Number



17. Was pre-dialysis/transplant EPO administered?

Yes No

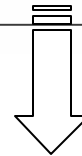
18. Laboratory Values Prior to First Dialysis Treatment or Transplant *See Instructions.

LABORATORY TEST	VALUE	DATE	LABORATORY TEST	VALUE	DATE
a. Hematocrit (%)			e. Serum Creatinine (mg/dl)		
b. Hemoglobin (g/dl)*			f. Creatinine Clearance (ml/min)*		
c. Serum Albumin (g/dl)			g. BUN (mg/dl)*		
d. Serum Albumin Lower Limit (g/dl)			h. Urea Clearance (ml/min)*		

B. COMPLETE FOR ALL ESRD PATIENTS IN DIALYSIS TREATMENT

19. Name of Provider

20. Medicare Provider Number



E. PHYSICIAN IDENTIFICATION

44. Attending Physician (Print)

45. Physician's Phone No.
()

46. UPIN of Physician in Item 44

PHYSICIAN ATTESTATION

I certify, under penalty of perjury, that the information on this form is correct to the best of my knowledge and belief. Based on diagnostic tests and laboratory findings, I further certify that this patient has reached the stage of renal impairment that appears irreversible and permanent and requires a regular course of dialysis or kidney transplant to maintain life. I understand that this information is intended for use in establishing the patient's entitlement to Medicare benefits and that any falsification, misrepresentation, or concealment of essential information may subject me to fine, imprisonment, civil penalty, or other civil sanctions under applicable Federal laws.

47. Attending Physician's Signature of Attestation (Same as Item 44)

48. Date

MM / DD / YY

49. Remarks

HIPAA Electronic Signature Standard

- ✍ ***Transportability and independent verifiability properties are critical***
 - *Signature versus mere Assertion about authorship / approval*
 - *Assertion sufficient in high trust environments*
 - *Does this apply to healthcare reimbursement transactions?*

- ✍ ***Digital signatures are transportable and independently verifiable***
 - *Potential to authenticate attached medical records without having to rely upon 'trust' in EDI submitter*

- ✍ ***For extended analysis, see***
 - *<http://www.tunitas.com/presentations/HIPAAEsigRule.zip>*

- ✍ ***Next NCVHS testimony on electronic signature scheduled for March 2005***
 - *Considered as part of E-Prescribing recommendation mandated by Medicare reform act.*

Esig Overview ~ Basic Questions

- ✍ **Why electronic signature?***
- ✍ **Where can electronic signatures be used?***
 - Regulatory and legal analysis*
- ✍ **How electronic signatures can best be created and maintained?***
 - Signature related risks and mitigation*
 - Role of Esig Policy*
 - Technology of electronic signature*
 - Speculating about HIPAA*
- ✍ **Case Studies***
- ✍ **Implementation Steps***

OnLine Health Plan Enrollment

✍ Blue Cross of California

- *“By checking boxes and entering my name below I am indicating my intent to electronically sign this application and warrant that all the information I have provided is true, complete and accurate”*
 - *Includes checkbox to authorize medical records release*
 - *Provides basis for termination should application be untrue or incomplete*

✍ Method supported by Blue Cross’ business risk calculation

- *Economic benefit of simplified transaction completion*
 - *Meet HIPAA and CA authorization and receipt of notice requirements*
- *Repudiation unlikely, ‘minimal’ downside to repudiation*
 - *Costs in processing application*
 - *Little potential harm to ‘impersonated’ applicant.*
 - *At worst, rejected for a health policy that did not apply for.*

EMR / EOE Signature

- ✍ **EMR / EOE signature technology choices are largely limited to a vendor's configuration options***
- ✍ **Vendor typically implements practitioner signature thru 'signature by computer code mechanism'***
- ✍ **Vendor specific schemes to ensure integrity of 'signature'***
 - Some very weak schemes leverage platform capability but may not satisfy security requirements*
 - E.g. signed records stored as MSFT Office documents, programmatically (VBA) invoking "Tools | Options | Security | Password to modify" functionality of Office*
 - Anyone with password can modify, so record not locked at time of signature*
 - MSFT does not intended only to prevent 'inadvertent' modification*
 - E.g. setting files as Read Only*
 - Administrator override*

EMR / EOE Signature (cont)

✍ Vendor liability concerns

- What are the consequences (to vendor) should there be a failure in the controls that ensure the integrity of signed records / orders*

✍ One vendor's solution is to apply the system's digital signature to a record once it is signed by practitioner

- Ensures long term persistence of the (practitioner) signature*
- Requires special controls over the invocation of system's signature key*
 - Prevent removal or invocation contrary to application policy*
- Digital signature is transparent to end users*

Electronic Prescription of Narcotic

- ✍ **Current DEA Rules require pharmacist to verify ‘original’ signature of prescribing physician before dispensing drug**
 - “Compelling government interest” in ensuring the authenticity of and accountability for narcotic prescription

- ✍ **Forthcoming rule will allow electronic prescription of narcotic if**
 - Prescription is digitally signed
 - Signer’s certificate from DEA approved CA
 - Must reference / comply with DEA certificate policy
 - Contemporaneous status check of certificate validity
 - Special protection requirements for (private) signature key
 - Biometric authentication of signer (physician) before key invocation !!!
 - Embed key in hardware module

- ✍ **DEA seeks to minimize ‘false assertion’ risk**
 - Reasonable implementation costs to be borne by regulated (organized medicine) sector

Patient Consent

- ✍ ***Large care provider capturing patient consents electronically***
 - *Capture patient's digitized signature using a variety of vendor 'signature pad' products and tablet PC*

- ✍ ***Consent record includes the digital signature of person obtaining the patient's consent (clinician, ADT clerk, etc)***
 - *Digital signature computed over document with attached patient signature*
 - *Provides a standards based method to ensure long term integrity of consent record*
 - *Avoid dependence on a variety of heterogeneous vendor solutions*

Continuity of Care Record

- ✍ **Continuity of Care Record (CCR) is an electronic record designed to track care given by a succession of providers**
 - E.g., an Electronic record provided by practitioner to hospital and subsequently to SNF
- ✍ **What sort of electronic signature will assure authenticity of CCR entries?**
 - CCR standard does not address security. The original source of CCR entries is a mere assertion.
 - Is 'source authentication' sufficient? Is it transitive?
 - In above example, can SNF rely upon hospital's assertion that practitioner 'authenticates' practitioner's CCR entries?
 - Are there limits to this transitivity?
- ✍ **Does the CCR requires a signature which is persistent, transportable and independently verifiable?**
 - Does it require a digital signature?
 - If so, then `xml_dsig` is natural choice for esig representation.

Esig Overview ~ Basic Questions

- ✍ ***Why electronic signature?***
- ✍ ***Where can electronic signatures be used?***
 - *Regulatory and legal analysis*
- ✍ ***How electronic signatures can best be created and maintained?***
 - *Signature related risks and mitigation*
 - *Role of Esig Policy*
 - *Technology of electronic signature*
 - *Speculating about HIPAA*
- ✍ ***Case Studies***
- ✍ ***Implementation Steps***

Application Design

✍ Requirements review

- Applicable state regulation*
- Important business partners / payers; e.g. Medicare COP*
- User community; especially practitioner input*

✍ Use case analysis

- Attention to constraints of the supported applications*

✍ Risk analysis

- What is the dispute resolution process?*
- What are the consequences of repudiation?*
- What is the value of the transaction?*

✍ Security design

- Lifecycle of credentials used for signature (creation issuance, storage, use, destruction)*
- Signature representation viewed from the perspective of 'preservation of evidence'*

Some Implementation Decisions

✍ Amendment and Correction

- Any constraints on changes to record prior to signature?*
- Who has responsibility of making changes to documents prior to signature?*

✍ Multiple document signatures

- Constraints on signer's as a function of role*

✍ Mandatory vs Optional use

- Optional use requires substantial duplication and process inefficiency, should seek to sunset 'optional' use asap*

✍ Management of multiple electronic signature systems

- Centralized vs decentralized management, deployment*

Validation

✍ Practitioner groups

- *Must be sensitive to physician workflow and liability concerns*
- *Update of Medical Staff bylaws as needed*

✍ State licensor where applicable

- *Some states require state approval before some (med records) types of E-SIGNuse*

✍ Trading partners where applicable

- *Especially where signed record will be submitted to payer or regulator*
- *Should be a negotiation. Both parties have interest in electronic submission;*
 - *Use threat of paper submission as bargaining chip*
 - *For Federal agencies, invoke Agency's obligation under GPEA*

✍ Enterprise legal

- *For any transaction involving consumers*
- *For high value transactions*

Rollout

*✍ **Role Appropriate Training (users, admin)***

*✍ **Workflow modification***

- As esig eliminates a paper process, workflow changes are required to ensure that efficiencies are preserved in transaction completion*
- Esig allows for ~~greater~~ different control over document release*

*✍ **Deficiencies***

- Electronic tracking of documents requiring signature*
- Manner of notification to practitioners*

*✍ **Contingency plan***

- What happens when esig system is not available?*

Maintenance

✍ Audit

- Documented review to ensure appropriate operation of signature controls*
- Without digital signature or ‘documented process’ there should be no expectation of ‘preservation of evidence’*

✍ Lifecycle of signature credentials

- Destruction; renewal; audit*

✍ Periodic assessment of business case parameters

- Meet or exceed expectations. Additional opportunity for process improvement*

Addendum

✍ Business Case Planning and Metrics

✍ Digital Signature Representation Formats

- Discussion regarding construction and use of the available standard formats for digital signatures*

✍ Further Resources

Building the Case

*✍ **Business Justifications***

- Identification of specific process targets*
- Identify success measures and set parameters*
- Relate target objectives to specific signature properties*

*✍ **Signature Method***

- Select a signature technology with the appropriate properties*
- Consider process improvement or workflow integration potential*

*✍ **Measure success factors in pilot project***

Forecasting the Benefit

✍ Types of return from Esig initiatives

- Increased compliance*
- More efficient process management*
- Reduced document costs*
- Greater transaction completion*

✍ Need metrics to quantify achievable benefit

Cost Minimization

- ✍ ***Typically, Esig costs are borne by the application creating the electronic record***
 - *Vendor solution administered as part of the application*

- ✍ ***Total costs may be minimized by centralizing some Esig functions***
 - *Authentication costs are reduced*
 - *reuse credentials across applications, simplified admin with greater enterprise control*
 - *Risk is reduced thru enterprise (rather than department) management and vetting of Esig scheme*
 - *Possible sharing of software components / signature capability*
 - *e.g. CCOW signature action agent which allows CCOW compliant clinical applications to share common Esig capability*
 - *e.g. AR's signature 'appliance'*

Increased Compliance

✍ Measurements

- Percent verbal orders meeting the 48 hr rule*
- Reduction in FTE performing signature chase*
- Reduction in redundant signature activity*
- Reduction in time to locate and pull records*

More Efficient Process

✍ Measurements

- Time to complete process*
- Time to retrieve documents*
- Percent of incomplete process after different periods*
- Customer satisfaction*
- User / staff satisfaction*
- Increase in quality of management reports*

Reduced Document Cost

✍ Measurements

- Cost of paper*
- Printing and delivery*
- Filing expense*
- Reproduction -- for archive and reimbursement*
- Re-allocated labor dollars*

Greater Transaction Completion

✍ Measurements

- Percentage transactions initialized but never completed*
- Revenue loss associated with incomplete transactions*
- Costs associated with tracking and follow-up*
- Increase in total transactions*

PKCS#7

- ✍ ***A data structure for encoding a digital signature***
 - *DER ('distinguished encoding rules')- 1st published 1993*
 - *Assumes only that the system can process an octet string*

- ✍ ***A PKCS#7 structure includes:***
 - *Version and algorithm information*
 - *Digital signature and manifest (optional)*
 - *Signer's X.509 certificate chain and contemporaneous CRL*
 - *Signer information (optional) including: signing date, signature purpose*
 - *ASTM E2084 standardizes healthcare specific signature attributes*

- ✍ ***Most commonly used digital signature representation***
 - *Many programmer tools (e.g. RSA, Baltimore, Microsoft)*

XML-Dsig

- ✍ ***W3C recommendation for XML representation of digital signature - adopted Feb, 2002***
 - *Important component of web services security*
- ✍ ***Generalizes PKCS#7 concepts***
 - *Defines a canonical form for document over which digital signature is computed*
 - *Optional representations of public key ownership*
 - *X509, PGP, SPKI, or directly exchanged key*
- ✍ ***Extensible***
 - *Supports a number of “SignerProperties” and other structure using standard XML namespace mechanisms*
- ✍ ***Readily available programming Tools available***
- ✍ ***Good fit with ASTM CCR and HL7 CDA standards***

DICOM Digital Signature Profile

- ✍ ***Intended to standardize definition of digital signature over radiological images***

- ✍ ***Defines***
 - *Different signer roles and signature purposes*
 - *Attributes included in the digital signature*
 - *Algorithms used in generating digital signature*

- ✍ ***Creates two distinct ‘secure use’ profiles***
 - *‘bit preserving’ digital signature use*
 - *Conventional understanding and use of digital signature*
 - *‘basic’ digital signature use*
 - *Validation of ‘incoming’ digital signature*
 - *Allows transformation / compression of validated incoming data object so long as it is stored in such a way that the object is guarded against ‘any unauthorized tampering’*
 - *Forwarding of the transformed data object, with digital signature defined over previously verified objects*

- ✍ ***For more info, see http://medical.nema.org/dicom/2003/03_15PU.PDF***

X12.58

✍ ***Defines internal X12 ‘control structures’ for source authentication and message integrity***

- *Supports digital signature of transaction set or function grouping of transaction sets*

✍ ***Implementation***

- *Requires that EDI application be ‘crypto aware’*
- *More difficult to implement than options, such as s/MIME, that are external to X12 message security*
- *Rarely implemented, but status may change*
- ***Federal Implementation Guidelines for EDI***
--NIST, July 2001
“The federal government is committed to providing security services for ASC X12 compliant EDI via the constructs provided by ASC X12.58.”
- *Will X12.58 be the HIPAA Final Security Standard?*

Useful References

✍ Healthcare Electronic Signature “Best Practice”

- ASTM e1762-95 (fee). Free draft of e1762 update by request to spankey@tunitas.com
- AHIMA Practice Brief “Implementing Electronic Signatures”
 - <http://www.ahima.org> and then use search engine
- FDA CFR 21 Part 11
 - http://www.fda.gov/ora/compliance_ref/part11/

✍ Legal / Regulatory

- American Health Lawyers (www.ahla.org)
 - Health Information and Technology Practice Guide (fee)
 - HIT mailing list
- State Codes
 - Links page: <http://www.edfoundation.org/ElectronicSignaturePolicy.htm>

✍ Developer / Standards Related

- PKIX WG <http://www.imc.org/ietf-pkix/index.html>
- xml_dsig WG <http://www.w3.org/signature>
- CAPICOM list: <http://discuss.microsoft.com/archives/capicom.html>
- OpenSource: <http://www.openSSL.org>