



Electronic Signatures – Overcoming Barriers to Efficient Healthcare

Patient safety, workflow inefficiencies and cost concerns are driving the healthcare organizations to greater reliance on electronic records and processes. New processes customized for electronic information and workflow, are needed to ensure critical document authenticity and integrity. Chief among these is a simple, effective means for recording and storing signatures.

Handwritten Signatures (Wet Ink)

A signature is a well accepted method for approving information and demonstrating its authenticity. Unsigned documents signal the process is incomplete or unauthorized. Where agreement or consent is required, an unsigned document indicates it has not been given.

Signatures on paper documents are simple to understand and execute. The signer is presented with the document, reads it, and if the content is complete, accurate and acceptable, signs the document. Once signed, the document can be copied, routed to other parties, stored in multiple locations and if additional original copies are needed, a notarized copy will usually suffice.

Applications

Patient Signatures

- Consents
- Discharge Instructions
- Advance Directives
- Administrative Requests

Physician Signatures

- Patient Orders
- Medical Records
- Medicare Certifications
- Business Agreements
- Business Correspondence

Employee Signatures

- Patient Documentation
- Business Agreements
- General Acknowledgements
- HR Enrollments

Corporate Signatures

- E-Transactions
- E-Acknowledgements
- E-Confirmations



Electronic Signatures

Healthcare organizations collect hundreds of signatures a day. Whatever means is used to replace paper-based signatures, it must be simple to use and easy to understand. That's why the prevailing trend for electronic signatures is the use of a graphical image of the signature and/or digital signatures.

How can we achieve the simplicity of hand signed paper documents for information maintained?

Although electronic and digital signatures sound the same, the two signature methods are very different and serve different purposes. Graphical image of the signature or for shorthand, graphical signatures, are an identical image of a person's handwritten signature. Graphical signatures have the advantage of being easy to capture, using any number of commercially available image signature pads. Graphical signatures are useful for many of the patient signatures that must be collected for informed consent, authorizations, admission enrollments, discharge instructions, healthcare directives and generally, any other type of electronic form.

This type of electronic signature is just a computer file which can be easily cut and pasted onto a number of documents and forms. This means it can be added to a document without the author's approval or knowledge. Both kinds of problems create risk that the signature will be found invalid. In the case of many types of healthcare signatures, an invalid signature can have significant consequences.

In contrast, digital signatures are commonly used to lock and seal the contents of a document. Digital Signatures (sometime referred to as Advanced or Secure Electronic Signatures) take the concept of the traditional paper based signature into the digital realm, by adding a digital "fingerprint" as a signature to a document. This "fingerprint" is unique to both the document and the signer.

The digital signature has the ability to uniquely bind the signer to the document's contents, ensuring data integrity and non-repudiation of the electronic transaction. Depending on the solution, any changes made to the document after it was signed are clearly indicated and invalidate the signature, thereby protecting against forgery.



When patients' signatures are required, a concept similar to a witness signature can take place. The patient signs using the signature pad. The graphical signature is captured and pasted onto the document, then the signed document is counter signed by a physician, with the later's digital signature.

The advantage of this two step approach is the high-degree of certainty that a document, once signed, has not been changed. The document and patient's signature are fixed together and can not be separated without detection. The resulting signed document is a single file that can be readily stored electronically, copied and distributed to others as needed for business purposes.

Computer Code Signatures

The early methods of electronic signatures have been primarily designed to authenticate the information maintained by a computer application. First used in the 1970s, these methods did not actually create a signature. Instead they required persons entering information to authenticate their identities by entering an assigned code. The application would only store the entered information, if the user's application ID matched the code number.

Signature by a computer code, as Medicare refers to this method, is only acceptable if the person using the code signs a formal agreement, called an attestation. Providing it is agreed that the code will be interpreted as their "electronic signature", kept secret, and not used for any other purpose or under no circumstances used by anyone else. Most electronic medical records systems still use the computer code method to authenticate electronic information.

Computer code signatures were reasonably acceptable for early electronic record systems, however are not capable of meeting the requirements of modern healthcare business needs. Their major advantage in the 70's has become their major disadvantage today. Since there is no actual signature, the authentication of the electronic information is strictly a function of how the application works and the security procedures used by the application owner to ensure that the information has not been changed or deleted. Effectively, this means that the information authenticity is not actually a function of the computer code signature.



Signature Requirements for Healthcare Applications

Today, health information is just as likely to be produced electronically as it is to be on paper. This means that information authenticity is a critical business property to ensure healthcare operations such as proper communication of patient information, physician orders, bills and payments and employment agreements. To meet these needs, signature technologists have defined the following set of signature properties:

Uniqueness - The property that ensures that an individual's electronic signature can be distinguished from that of any other person. Uniqueness is a core principle of any signature. Without uniqueness, a signature has no meaning. It's uniqueness ensures authorization, acceptance or approval.

Persistence - The property that allows signatures to be retrieved and verified at any time in the future. Signature verification must be possible even after the original application has been migrated through major system upgrades. Persistence is particularly important for healthcare records that may have extensive retention periods. Retrospective billing audits, peer review data, patient authorizations and consents are highly dependent on persistence authenticity.

Transportability - The property that allows signatures to be communicated across networks to third parties. This property is necessary in situations where the receiving party has a requirement to validate a signature. For example, certain Medicare claims require documentation of a signed certificate of necessity. Without transportability, electronic documents can be created and communicated, but the signature does not travel with the document.

Independent Verifiability – This is the property that allows a signature to be verified by the recipient independently without reference to an application maintained by another party. This property is closely related to persistence and transportability. Without independent verifiability, signatures communicated to third parties have little use or meaning.



Integrity - The property ensures that any modification made to the contents of the document after it has been signed will cause the electronic signature to be invalid or unverifiable. Like uniqueness, integrity is a core signature principle, without which a signature is meaningless. Many signature disputes arise over the principle of integrity. Signers don't disclaim their signature, rather they maintain the document or information is different from that at the time they signed. Signature (or information) integrity is highly dependent on technical controls and security procedures.

Non-repudiation - The property that describes the ease with which a signer could falsely disclaim responsibility for the signed information. Non-repudiation is not yet a high priority for most healthcare signatures. This is because common practice describes when signatures are required and business procedures are implemented to ensure that required signatures are collected. However, as more healthcare operations become automated, signatures will become a critical component of managing workflow and authenticating procedures.

Comparing Different Electronic Signature Methods

	Traditional Computer Code Signatures	Graphical Signatures	Digital Signatures
Signature Uses	<ul style="list-style-type: none"> Medical records 	<ul style="list-style-type: none"> Patient or employee forms 	<ul style="list-style-type: none"> Witness or counter signatures Integrity authentication Transactions Email Web applications
Signature Properties	<ul style="list-style-type: none"> Uniqueness 	<ul style="list-style-type: none"> Uniqueness Persistence Transportability 	<ul style="list-style-type: none"> Uniqueness Persistence Transportability Independent Verifiability Integrity Non-repudiation
Advantages	<ul style="list-style-type: none"> Traditional method Accepted for physician signatures 	<ul style="list-style-type: none"> Becoming a standard consumer method Low cost signature pads Good for where signature is backed by credit card or other authorizing method. 	<ul style="list-style-type: none"> Becoming the preferred method for e-transactions, corporate signature uses, legal documents and integrity authentication Works for all kinds of signature applications Supports all signature properties
Disadvantages	<ul style="list-style-type: none"> Costly to administer Subject to code sharing No integrity properties Cannot be used outside of an application Does not standardize 	<ul style="list-style-type: none"> Signature is not fixed to information or document Signature can be cut and pasted onto any document 	<ul style="list-style-type: none"> Early products were expensive and costly to administer Resistance by application vendors to migrate away from computer code signatures



Digital Signatures – The Best Practice Method for Sealing & Authenticating Electronic Documents

Digital signatures are well recognized as the preferred method of sealing & authenticating electronic documents. That's because they provide all the signature characteristics that a healthcare organization needs to replace its dependence on paper and handwritten signatures. The value and benefits of digital signatures are promoted by a number of influential organizations.

“Digital signature technology generally surpasses paper in meeting the attributes necessary to authenticate a legal transaction.”

-- ABA Digital Signature Guidelines Tutorial

The American Bar Association endorses digital signatures and has published a comprehensive set of guidelines for authenticating documents using digital signatures. The federal government has standardized its use of digital signatures and now requires them for many types of electronic transactions. The Drug Enforcement Agency (DEA) has just released its draft regulations requiring the use of digital signatures for authenticating electronic prescriptions. The Veteran's Health Administration digital signatures for integrity control over patient consents and forms. Standards for using digital signatures for healthcare purposes are already being published. There is an ASTM standard for using digital signatures to authenticate medical records and a DICOM standard under development for digitally signing radiological images.

The Power of CoSign

CoSign is a simple to use and quick to deploy digital-signature solution from ARX. CoSign delivers an innovative solution for digitally signing documents, files, forms and

The innovative way to digitally sign electronic transactions, documents and forms just as you would on paper.

transactions. It is designed to “sit” on the corporate network and operate as a signature service.

This means that all the advanced technology is hidden from users.

Whenever a signature is required,

the user simply clicks the sign icon. The data file, document or form is sent to CoSign which identifies the individual's signing key, adds the signer's graphical signatures, digitally signs the information and returns it back to the individual.

CoSign eliminates the overhead expenses typical with other solutions due to its unique centralized approach for generating, storing & managing private keys, built-in integration with the organization's existing User-Management-System and wide 3rd party application support. CoSign also supports high availability and high-volume batch signing offerings.



CoSign Delivers

Sealed documents – Locks documents and data against any changes including forging attacks while maintaining "business as usual" processes. Any changes made to the document are clearly indicated and invalidate the signature, thereby protecting against **forgery**, as each signature is uniquely linked to the signer.

Standardized signature method – CoSign uses industry standard Digital Signatures based on "Public Key Infrastructure" (PKI) technology for signing and validating signatures. Using these standards allows receiving parties to validate signatures without requiring additional software installation (in supporting applications).

Smartcard-free solution - Eliminates the need and costs associated with Smartcards.

Quick ROI – Simplifies signature procedures and improves your user's satisfaction.

Automate & Expedite Processes - Accelerate your transition to electronic records. As a result, increases employee efficiency and enhances patient service.

*Whether you are concerned about patients' privacy, electronic digital signature capture, legal electronic documents, document scanning, improved scheduling, patient recall, HIPAA compliance, insurance audits, risk management or security, **CoSign offers an affordable and easy to use solution for you.***

Seamless, secure, and easy to use, CoSign lets you digitally sign, records with the click of a mouse. For more information on CoSign digital signatures visit www.arx.com/CoSign.html



For more information please contact sales@arx.com or visit www.arx.com

Your comments and feedback are welcomed media@arx.com

