

Digital/Electronic Signatures for Medical Records

May 2008



Simple
Valuable
Affordable

Introduction

Healthcare organizations are increasingly relying on digital signatures (standard electronic signatures) for medical records as a way to improve patient safety, workflow inefficiencies, and cost concerns. Medical records digital signatures are a simple, effective means for recording and storing signatures while ensuring critical document authenticity and integrity.

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

Table of Contents

Introduction	2
Handwritten Signatures (Wet Ink)	2
Digital Signatures for Medical Records - Overcoming Barriers to Efficient Healthcare	3
Properties of a Digital Signature	4
Computer Code Signatures	4
Signature Requirements for Healthcare Applications	5
Comparing Different Electronic Signature Methods	6
Digital Signatures - The Best Practice Method for Sealing & Authenticating Electronic Documents	6
The Power of CoSign	7
CoSign Delivers	7
About ARX	8

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 a document, and if the content is complete, accurate and acceptable, they sign the document. Once signed, the document can be copied, routed to other parties, and stored in multiple locations. If additional original copies are needed, a notarized copy will usually suffice.

Digital Signatures That Keep Your Business Moving

Digital Signatures for Medical Records - Overcoming Barriers to Efficient Healthcare

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

Although electronic and digital signatures sound similar, the two signature methods are very different and serve different purposes. A graphical image of the signature (graphical signatures) is 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 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.

A graphical signature is a simple computer file that can be easily cut and pasted into a number of documents and forms. This means it can be added to a document without the author's approval or knowledge. These signatures can create a risk that the signature will be found invalid. As it relates to the healthcare industry, an invalid signature can have significant negative consequences. So while graphical signatures may seem to be a simple signing solution, they have significant inherent drawbacks.

Digital signatures are commonly used to lock and seal the contents of a document. Digital signatures (sometimes 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 properties of a digital signature are quite simple. A 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 with digital signatures. The patient signs the document using the signature pad to create a graphical signature. The graphical signature is captured and pasted onto the document, then the signed document is counter-signed by a physician, with the healthcare employee's digital signature.

The advantage of this two step approach is the 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.

Properties of a Digital Signature

Digital signatures are commonly used to lock and seal the contents of a document. Digital signatures (sometimes 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 properties of a digital signature are quite simple. A 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.

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

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 latter'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 digitally, copied, and distributed to others as needed for business purposes.

Computer Code Signatures

The early methods of electronic signatures were 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. An attestation provides that the code will be interpreted as the individual's "electronic signature", kept secret and not used for any other purpose, or 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, they are not capable of meeting the requirements of modern healthcare business needs. The major advantage of computer code signatures of the 1970's has become their major shortcoming 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, payments, and employment agreements are accurate. 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. Its 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 do not 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 into 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 and authenticating electronic documents. That is 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.

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

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

- ABA Digital Signature Guidelines Tutorial

Digital Signatures That Keep Your Business Moving

prescriptions. The Veteran's Health Administration utilizes 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 transactions. CoSign 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.

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

CoSign eliminates the overhead expenses typical with other digital signature solutions due to its unique centralized approach for generating, storing, and managing private keys, its 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

- ▶ **Accelerated Business.** CoSign accelerates the pace of doing business electronically with customers, partners, and prospects by sharing quick, easy, and secure transactions and records between firms and across geographies. CoSign is convenient and handles high-volume transactions for any size business with ease. The CoSign PSF is based on industry standards and boasts technical compatibility with a broad set of applications to guarantee electronic signature records can be easily read and verified for decades.
- ▶ **Lower Costs.** CoSign allows users to reduce costs associated with authorizing and signing documentation. It also reduces the costs and quality challenges associated with archiving, audits, and legal requirements. By reducing costs associated with traditional paper-based processes (i.e., paper, printing, ink, scanning, faxing, postage, and processing time), organizations realize a quick Return on Investment (ROI).
- ▶ **A Simple Click.** CoSign makes it easy to sign, verify, and retain digital records because the digital signature standard is already built into applications like Microsoft® Word, Excel®, SharePoint®, Outlook®, Adobe® Reader®, Acrobat®, AutoCAD®, IBM Lotus®, Oracle UCM, and Lawson M3, among others. Because of this, CoSign users simply sign with one click using familiar applications.
- ▶ **No Vendor Lock-In.** By using a standards-based digital signature technology, CoSign digital signatures transform signed documents into portable electronic records that are maintained in a non-proprietary

Whether you are concerned about patient 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.

Digital Signatures That Keep Your Business Moving

format. This allows third-party document recipients to easily verify signatures in commonly used applications without costly, complicated, or proprietary software.

- ▶ **Document Integrity.** CoSign seals documents digitally, verifying the document has not been altered after signing, providing proof of the signer's identity, intent, and document integrity over the life of the document record.
- ▶ **Legal and Regulatory Compliance.** CoSign digital signatures enable organizations to comply with regulations worldwide, including: FDA Title 21 CFR Part 11, HIPAA, US E-Sign (Electronic Signatures in Global and National Commerce Act), EU Directive for Electronic Signatures, and the EU's VAT Directive.

About ARX

ARX (Algorithmic Research) is a global provider of cost-efficient digital signature solutions for industries such as life sciences, healthcare, government, engineering, and manufacturing industries. ARX engineers and scientists have more than 20 years experience in security and standard digital signature application. ARX helps businesses secure, streamline, and scale their business processes and transactions with the proper controls required by legislation, regulation and industry best practice. Visit us at <http://www.arx.com>.

Digital Signatures That Keep Your Business Moving