

CoSign for 21 CFR Part 11 Compliance

March
2007



Digital Signatures **Made Simple**

Secure
Simple

Electronic Signatures at Company XYZ

Company XYZ operates in a regulated environment and is subject to compliance with numerous US government regulations governed by the Food & Drug Administration (FDA) and HIPAA.

This document is provided to explain the use of the digital signatures on various documents at Company XYZ business operations. For all digitally signed documents at Company XYZ, the electronic version stored on the network or in a database is considered the *source* document and all printed documents are for working use only.

FDA and HIPAA Electronic Signature Requirements

There are no specific requirements by the FDA or HIPAA to use electronic signatures, however both agencies/departments accept electronic signatures to be used in a compliant manner.

FDA. The U.S. Food and Drug Administration's 21 CFR Part 11 Electronic Records, Electronic Signatures - Final Rule (March 20, 1997) and the FDA's Guidance for Industry, Part 11, Electronic Records, Electronic Signatures—Scope and Application (February 4, 2003) are the guiding Predicate Rules for this market.

The 21 CFR Part 11 areas covered by the system include:

- 11.10 Controls for closed systems
 - (d) Limiting system access to authorized individuals.
 - (e) Audit trails.
 - (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
- 11.30 Controls for open systems
 - Authenticity & integrity of electronic records from the point of their creation to the point of their receipt.
- 11.50 Signature manifestations
 - Signed electronic records shall clearly indicate printed name of signer, date & time and reason for signing.
- 11.100 General requirements
 - (a) Unique electronic signatures for each user.
- 11.200 Electronic signature components & controls
 - Employ at least two distinct identification components; Continuous sessions.

HIPAA. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) prompted new federal regulations which require physicians to ensure they are protecting the privacy and security of patients' medical information and using a standard format when submitting electronic transactions.

The HIPAA Security Standards require physicians to protect the security of patients' electronic medical information through the use of procedures and mechanisms that protect the confidentiality, integrity, and availability of information. Physicians must have in place administrative, physical, and technical safeguards that will protect electronic health information that the physician collects, maintains, uses, and transmits. The compliance date for the Security Standards was April 20, 2005.

PKI Based Digital Signature Technology

Company XYZ achieves FDA 21 CFR Part 11 and HIPAA Security Standard data integrity compliance through the use of digital signature technology similar to the same PKI based systems used throughout the US Federal Government.

In order to gain a deeper understanding of PKI technology, the reader is encouraged to refer to the widespread literature published on the subject. A good starting point would be the PKI forum at www.oasis-pki.org or the Federal PKI Steering Committee site at www.cio.gov/fpkisc.

PKI based digital signatures are the only standard for electronic signatures in the world today. PKI provides each user (signer) with a key-pair, a Private Key and a Public Key used in every signature. The Private Key, as the name implies, is kept private and stored securely; the Private Key is used for signing, thereby adding a digital "fingerprint" to the document. The Public Key (from which the Private Keys were created) is made widely available to any person who wishes to use it for validating the sender's digital signature.

The value of digital signatures from an electronic record standpoint is that signed documents "stand on their own" as self-contained, portable, electronic records. Recipients anywhere in the world simply open the signed document (the Private Key is hashed to the document) in order to verify the contents authenticity (who signed) and data integrity (what was signed). Hence, signed documents can be used as electronic evidence for audits to prove unique ID and intent of signer and guarantee that the data has not been altered since the signature was added.

Company XYZ Digital Signature Solution

Company XYZ uses a digital signature solution named CoSign® from Algorithmic Research, Inc (ARX).

CoSign provides all of the features of PKI Based Digital Signatures described above, plus it provide additional features as required by 21 CFR Part 11. For example:

- All digital signatures include the user's full name, a time/date stamp and force a "reason for signing" to be entered. The digital signature also includes the display of the "graphical" or handwritten signature of the individual. In addition, the digital signatures contain a wealth of information about each signer in the certificate of each signer contained in the digital signature.
- The Private Keys (used for signing) and associated certificate (used for identification) are stored in a security appliance being certified by National Institute of Standards and Technology (NIST) / National Security Agency (NSA) for "Common Criteria Evaluation and Validation Scheme" under one of the highest level security profiles, as well as the older FIPS 140-2 Level 3 certification. Hence, the digital signature keys and certificates are secure.
- The digital signatures can only be applied after the user successfully authenticates using a unique two form Username plus Password combination.
- Each digital signature in a document covers a defined scope (partial or entire documents); reviewers can verify that the data covered by a signature has not been altered since the signature was applied. Each signature operations is stored in a log in the secure CoSign device. Certain file formats, such as PDF, also provide a full audit log or revision history associated with each contained signature; the exact status of the document contents can be viewed at the time of which each signature was applied.

The CoSign system has been used in many FDA regulated applications including hundreds of clinical trials for compliance with various GxP, Computer System Validation, and regulatory documentation; and over one hundred times for Vendor and FDA Audits.

For HIPAA Security Standard data integrity requirements, each digital signature in a document "seals" as defined scope (partial or entire documents); reviewers can verify that the data covered by a signature has not been altered since the signature was applied (validating whether the "seal" was broken). Because the CoSign digital signatures are standard PKI, the system also provides a mechanism for "portability" of medical records by enabling the signed documents to be routed to recipients inside and outside of the organization for

Digital Signatures Made Simple

verification (check Who/When/Why/What was signed) without any proprietary hardware or software other than the signed document plus the Public Key (root certificate of XYZ Company) to perform this task.

Related Policies and Procedures

Company XYZ Electronic Records System

To minimize the risk of a signed document accidentally being changed within Company XYZ; a digitally signed document is moved and stored into an appropriate directory which has '*create and read only*' rights. The source document is controlled in accordance with documented procedures, the same as for all electronic records that are subject to regulatory requirements. These procedures include backup and archiving.

Identity Proofing

Company XYZ has procedures in place to ensure that the identity of the individual has been established before they are setup and given the ability to use the digital signature system.

Since the electronic signature system is being used only by *internal* users, Company XYZ has an employee policy in place that describes the accepted use of digital signatures. In order for the CoSign system to generate a Private Key and certificate for an individual, that individual needs to be approved and entered into the Company XYZ employee database (Microsoft Active Directory system).

Company XYZ informs all users that the digital signatures are intended to be a legally binding equivalent of traditional handwritten signatures in accordance with 21 CFR part 11 clause 11.100 c.