

# CoSign Digital Signatures and HIPAA

## Overview

HIPAA ([Health Insurance Portability and Accountability Act of 1996](#)<sup>1</sup>) is a set of regulations developed by various government agencies and members of the health industry. It's designed to protect patient rights, and simplify the process of passing authorized information from one approved industry entity to another. HIPAA contains a set of standards to be used by all agents of the industry with regard to how the information is transferred and protected.

## Regulations

Discussed below are the three main provisions of this Act and the role ARX's CoSign® digital signature solution plays with regards to compliance.

- ▶ **Transaction Standards:** The transactions standards call for use of common electronic medical claims standards, common code sets, and unique identifiers for all healthcare payers and providers. This provision does not involve or impact electronic and/or digital signatures.
- ▶ **Privacy Regulations:** The privacy rules govern the release of individually identifiable Personal Health Information (PHI), specifying how health providers must provide notice of privacy policies and procedures to patients; obtain patient consent and authorization for use of information; inform patients how information is generally shared; and inform patients how they can access, inspect, copy, and amend their own medical record. The potential use of electronic signatures under this regulation is addressed in the [Privacy and Security Framework Guidance Documents](#)<sup>2</sup> as follows:
  - ▶ **Transparency Principle:** The Privacy Rule generally requires that covered health care providers with direct treatment relationships with individuals provide a copy of the Notice of Privacy Policy (NPP) directly to the individual on the date the first service is provided, and make a good faith effort to obtain the individual's written acknowledgment of receipt of the NPP. The guidelines further specify that the NPP can be provided electronically. CoSign digital signatures can be used to demonstrate compliance with privacy regulations by capturing the patient's signature on a Notice of Privacy Practice (NPP) acknowledgment form or on the NPP itself.
  - ▶ **Individual Choice Principle:** Covered entities are required to obtain a patient authorization for any use or disclosure of PHI not otherwise expressly permitted or required by the Privacy Rule. In addition, the Privacy Rule allows covered entities to obtain the individual's consent in order to use or disclose PHI for treatment, payment, and health care operations purposes. Individuals also have the right to request restricted uses or disclosures of PHI.

CoSign digital signatures can be used to demonstrate compliance with privacy regulations by capturing the patient's signature on authorizations, consents, and disclosure restriction requests.

- ▶ **Safeguards Principle:** The Privacy Rule requires covered entities to verify the identity and authority of a person requesting PHI, if not known to the covered entity. The guidelines specifically state, "Documentation requiring signatures may be provided as a scanned image of the signed documentation or as an electronic document with an electronic signature, to the extent the electronic signature is valid under applicable law."

<sup>1</sup> <http://aspe.hhs.gov/admsimp/pL104191.htm>

<sup>2</sup> <http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/>

CoSign digital signatures can be used to demonstrate compliance with privacy regulations by demonstrating review and approval of requests for Release of Information, as well as by authenticating the identity of the requestor.

- ▶ **Security Regulations:** The Security regulations dictate how the electronic information used by the healthcare industry should be stored, transferred, and used to ensure the privacy of individually identifiable PHI. Specifically, the Security Rule addresses confidentiality, integrity, and availability of PHI. Further, the Security Rule requires that providers establish and maintain administrative, physical, and technical safeguards to protect PHI.

The potential use of Electronic Signatures is treated as a Technical Safeguard in the [HIPAA Security Standard Final Rule 45 CFR Part 164.312](#)<sup>3</sup> as follows:

- ▶ **Part 164.312(c)(1), Integrity Standard:** Organizations are required to implement policies and procedures to corroborate that data in their possession have not been altered or destroyed in an unauthorized manner.

In their commentary on this standard, the regulations state, "We believe that this standard will not prove difficult to implement, since there are numerous techniques available, such as processes that employ digital signature or check sum technology to accomplish the task."

The CoSign Digital Signature application employs Public Key Infrastructure (PKI) technology to encrypt the signed document or data and corroborates that the signed data has not been altered. In addition, CoSign requires user authentication via centrally-managed identification certificates in order to sign the document, ensuring that only authorized signers are sealing the document.

- ▶ **Part 164.312(e)(2), Transmission Security Standard:** Organizations are required to implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

The CoSign Digital Signature application simplifies compliance of this section by creating a portable signature record that cannot be tampered with or modified without detection.

## Conclusion

With regards to Privacy Regulations, the CoSign digital signature solution helps a healthcare entity to implement and enforce the privacy policies it makes public. It can demonstrate compliance with patient notification requirements as well as appropriate review of requests for protected health information.

With regards to Security Regulations, the CoSign digital signature solution not only meets the HIPAA requirements as presented in the Final Rule 45 CFR Part 164.312, but also meets the more specific and restrictive requirements of the earlier [Proposed Rule 45 CFR Part 142.310](#).<sup>4</sup> Further, CoSign meets the most restrictive Electronic Signature and Electronic Record requirements as mandated by the Department of Health and Human Services for use by the FDA in Rule 21 CFR Part 11. The ARX CoSign product is the largest and most widely deployed digital signature system in the FDA-regulated marketplace.

Ultimately, HIPAA Regulations compliance is the responsibility of the healthcare organization and is the result of processes and procedures that make use of security features in the CoSign applications. ARX encourages review of internal processes to ensure organization policies meet the guidelines of HIPAA regulations.

<sup>3</sup> [http://www.access.gpo.gov/nara/cfr/waisidx\\_07/45cfr164\\_07.html](http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr164_07.html)

<sup>4</sup> <http://aspe.hhs.gov/admsimp/nprm/sec13.htm>