CERTINAL

ACHIEVE SEAMLESS INTEROPERABILITY IN THE HEALTHCARE INDUSTRY

The ultimate guide to HIPAA-compliant digital signature you'll ever need

Index

Introduction:

Many administrative procedures in the healthcare sector have been demonstrated to be more effective when using digital signatures. Yet, some healthcare organizations need clarification on the HIPAA e-signature standards.

Do digital signatures satisfy the **HIPAA criteria,** and are they equal to patients signing paper documents? It is acceptable for HIPAA-covered entities and business associates to use digital signatures as evidence that a person has read and agrees with the contents of documents if specific safeguards are put in place to guarantee the validity and security of the contract, record, agreement, or authorization. There is no risk to the integrity of (Protected health information) PHI.

Understanding HIPAA - Health Insurance Portability and Accountability Act

Understanding HIPAA - Health Insurance Portability and Accountability Act

Maintaining **HIPAA compliance** is essential and mandated by law. The Health Insurance Portability and Accountability Act (HIPAA), a U.S. federal law, was passed in 1996 and called for "the development of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."

Protected health information (PHI) is the term used in this context to refer to patient data, including private health information like demographics, medical history, lab results, and insurance details. Only HIPAA-covered entities can receive this data for healthcare services, administration, and payment. Software platforms must sign a Business Associate Agreement outlining and confirming their commitment to protecting PHI before being used by HIPAA-covered entities. **Certinal eSign's** enhanced threat prevention keeps patient PHI secure and assures HIPAA compliance.

The 2003 Security Rule's initial draft included provisions for employing e-signatures under HIPAA Rules; however, those provisions were removed before the Act was passed. The U.S. Department of Health and Human Services website contains more recent advice about Business Associate Agreements and the interchange of electronic health information that states: "No standards exist under HIPAA for electronic signatures. Covered entities must ensure that any electronic signature utilized will result in a contract that is enforceable under applicable State or other laws in the absence of particular criteria.

Ignoring HIPAA Compliance Is a Huge Gamble

Ignoring HIPAA Compliance Is a Huge Gamble

The **HITECH Act** was passed to provide funding for the use of computerized EHRs by the healthcare infrastructure. However, it also broadens the application of HIPAA and adds new security and privacy obligations, such as:

01 Notifying the public of security lapses:

Giving notification to people and media organizations falls under this. Thorough information about the breach must be given to each impacted person and the Department of Health and Human Services if unsecured PHI is "accessed, obtained, or exposed" by or to an unauthorized person. The notice must be issued in well-known media outlets serving the State if the breach affects more than 500 citizens of that State.

02 Stricter PHI request accounting and compliance:

Healthcare providers must let people know when they are giving them ePHI if they ask for it. They must also maintain a thorough record of every time a patient's PHI is shared to receive treatment, make a payment, or conduct other medical procedures.

03 Stiff fines for infractions:

The Department of Health and Human Services (HHS) may be compelled to impose penalties up to $50,000 per violation of HIPAA or the HITECH Act if the infringement resulted from deliberate neglect; there is no maximum penalty for numerous cases of abuse. Although the word "willful disregard" is not defined, it might be argued that this criterion will apply whenever the protections and procedures mandated by law are not implemented. If the infraction is not the product of purposeful neglect or is remedied within 30 days of its discovery, less severe sanctions may be applied.

04 Additional accountability for business partners' Protected health information (PHI) management:

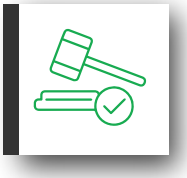
Recent allegations of data breaches at medical facilities are attributed to insufficient controls at commercial partners. As a result, the HITECH Act now mandates that healthcare organizations specify and approve the use of PHI in their business associate contracts. Healthcare institutions, service providers, vendors, or any other company handling PHI may be considered business associates. Your organization will be able to prioritize the assessments and particular requirements for your business associates by using a risk-based assessment to identify which associates present the highest breach risk.

Conditions Required for digital signatures under HIPAA Rules

Conditions Required for digital signatures under HIPAA Rules

Digital signature solutions are a terrific method to simplify paperwork procedures, whether protecting sensitive patient health information or satisfying physician signature requirements on medical documents. But first, covered entities like healthcare organizations must carefully select a PHI-protecting solution.

To be utilized per HIPAA regulations, digital signature systems must fulfill the following requirements:

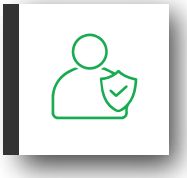


Legal Compliance -

The document provided for signature must adhere to federal laws governing eSignatures, clearly describe the terms and the signatory's intent, and give the signer the choice of receiving an emailed or printed copy of the signed document.

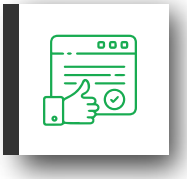
User authentication -

There must be a way to confirm the identity of everyone who signs documents; examples include two-step verification, password security, or security questions.



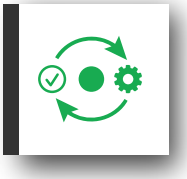
Message Integrity -

To prevent tampering with or to modify a signed document, security measures like encryption must be in place.



Non-Repudiation -

To be admissible in court, there must be a time-stamped audit trail that includes the dates and times of the signings, the chain of custody, and the location.



Ownership and Control -

For covered entities to store digital documents, all evidence of eSignatures must be in their possession.

What to look for in a digital signature solution to ensure it supports HIPAA compliance

What to look for in a digital signature solution to ensure it supports HIPAA compliance

Only some e-signature methods are the same. Therefore, when assessing potential technologies, it's crucial to consider the vendor's security, data protection, and storage approach.

Storage of data and encryption:

Every organization has a different appetite for risk security, influenced by how the industry functions and the corresponding legal and regulatory requirements. However, security is a top priority for all HIPAA-covered entities regardless of the industry, and the proper handling of data is essential to maximizing protection.

What should you look for?

A minimum of 256-bit encryption

The security protocols they employ, e.g., HTTPS, SSL, SSH, IPsec, SFTP

What data/documents do they encrypt

What cipher suites do they support

Whether or not they provide non-repudiation for all generated and signed documents

If they have a data disposal and reuse policy

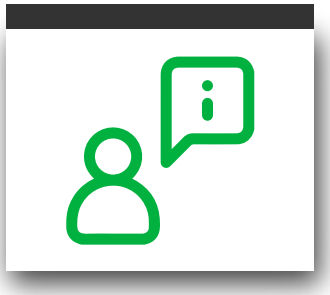
What processes do they have in place for equipment management and secure media disposal

Data Privacy:

It all comes down to safeguarding user data, like classification, storage, and encryption. Does the company offering the e-signature solution have a privacy program? Can it withstand the scrutiny required to meet the most stringent regulations governing the healthcare industry? Additionally, if any of your patients reside in California, you must confirm that the vendor complies with the California Consumer Privacy Act.

Considerations:

How is sensitive data handled, such as personally identifiable information (PII) and protected health information (PHI)?



Whether or not consumers have the choice to opt-in or out of getting information?

How is personal data being used?

Benefits of using a HIPAA-compliant digital signature

Healthcare firms may become more efficient thanks to digital signatures by digitizing their document workflows and quickly capturing and storing patient data online. However, even when handling signature workflows cannot be done in person, as is frequently the case during the epidemic, it is crucial to keep them going. Certinal uses dual authentication, encryption that meets federal agency standards, and thorough Audit Trails to safeguard sensitive medical data.

Common questions regarding HIPAA and the use of digital signatures

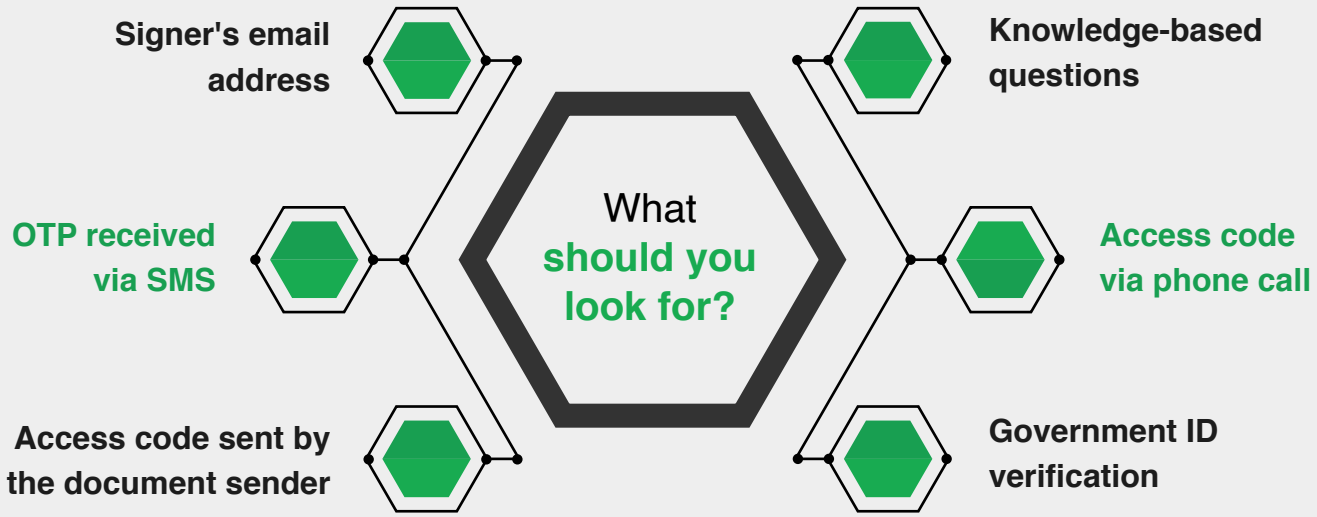
Common questions regarding HIPAA and the use of digital signatures

Is it legal to sign electronically under HIPAA?

Yes. HIPAA requires no specific method of signing documents. The law is instead concerned with making sure PHI is adequately handled.

What level of authentication is necessary to keep HIPAA compliant?

Depending on your business needs and practices, your organization will need a certain level of authentication. Before a signer can access the document and sign it, e-signature technology provides several options for confirming their identity, including:



Some suppliers offer two more degrees of e-signature that are compliant with the E.U.'s eIDAS criteria for circumstances when different levels of signature validity are required:

AES

Identity verification is necessary for AES. A signature must be able to identify the signer and be uniquely linked to them.

QES

Face-to-face identity verification is necessary for QES. A live, in-person, or audio/video connection can be used for face-to-face identification. A QES is distinctive in that the E.U. regards it as having the same legal standing as a handwritten signature.

Are medical forms with electronic signatures admissible as evidence in court?

In the U.S., electronic signatures are recognized by law. **The U.S. Electronic Signatures in Global and National Commerce Act (ESIGN, 2000)** and the **Uniform Electronic Transactions Act (UETA, 1999),** ratified by the majority of state legislatures, are the two main Acts that establish the legality of electronic signatures. Both ESIGN and UETA prove that electronic records and signatures have the same legal significance and effect as written signatures and conventional paper documents. "A document or signature cannot be denied legal effect or enforceability merely because it is in electronic form," the ESIGN Act states.

Can I integrate e-signature technology with my current EHR system?

Several technologies enable the automatic upload of electronically signed patient forms back into an Electronic Health Record (EHR) system from where they were initially sent. Organizations can take strategic steps to enhance the patient intake and consent process while maintaining HIPAA compliance by implementing e-signature technology outside of the EHR.

How does Certinal enable HIPAA-compliant document signing?

How does Certinal enable HIPAA-compliant document signing?

Certinal is dedicated to safeguarding your data and assisting healthcare clients in adhering to regulatory obligations. Every medical document you fill up and sign on Certinal complies with HIPAA security requirements. Certinal eSign ensures secure storage and transmission of sensitive medical information through password protection, 256-bit encryption, and SOC 11 Type 2 certification. The court-admissible Audit Trail of Certinal tracks the signing date, time, and place and all document modifications. Additionally, Certinal ensures that all documents can only be digitally signed by those who can do so.

Healthcare organizations must make it simple for patients to sign intake and consent forms wherever they are in the digital and remote world of today. **The Certinal eSignature for Certified EHRs** allows patients to electronically complete their intake forms from any location. These documents will automatically be uploaded into the EHR or your document management system after being completed electronically, with or without a manual review. Learn more about Certinal's healthcare-specific solution.

Intrigued to know more about how Certinal can improve patient care?

Book a demo or write to us at

switchto@certinal.com

Certinal is a wholly owned subsidiary of Zycus, the pioneer in Cognitive Procurement. A familiar name and market leader with years of experience in managing critical contracts & agreements, Zycus boasts of over Fortune 1000 enterprise clients and deployments of procurement and sourcing suite of products. Digital Signing has always been a focus area for Zycus. Thus, Certinal was born with the stated goal of offering a best-in-class Digital Transaction Management solution that will be easy-to-usetouse secure to deploy, and legally compliant around the world. We stand committed to providing a one-stop solution to large enterprise customers, compliant with various security standards and conforming to different regional regulations.

---

919 North Market Street Suite 950, Wilmington, New Castle County, Delaware - 19801

www.certinal.com