DocuSign®

eBook

# Using E-Signature to Help Manage HIPAA Compliance

For healthcare patients, filling out consent forms, insurance forms, privacy releases and other paperwork by hand can be one of the most tedious, frustrating parts of visiting a healthcare provider. Patients expect and want a digital experience.

Manual, paper-based processes negatively impact healthcare providers, too, because it takes their time and attention away from higher value activities, including interacting with patients.

Driven by patient expectations and a desire to improve productivity and cost-efficiency, many healthcare organizations are exploring technologies like electronic signature for patient forms. Providers also typically want and need a solution that complies with the Health Insurance Portability and Accountability Act (HIPAA).

This eBook provides guidance and answers to common questions regarding HIPAA and other regulations governing the use of electronic documents and signatures in healthcare organizations.

## HIPAA Overview

The U.S. Department of Health and Human Services (HHS) established two directives following the passage of HIPAA: the HIPAA Privacy Rule and the HIPAA Security Rule.

### Privacy Rule

Outlines standards for Protected Health Information (PHI) which includes information such as demographic data, medical history, insurance details and lab results.

### Security Rule

Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information.

# Common questions regarding HIPAA and the use of electronic signatures

## Is electronic signature allowed under HIPAA?

Yes. HIPAA does not mandate that documents be signed in a particular way. Instead, the law is focused on ensuring PHI is handled properly.

## How can e-signature help healthcare providers manage HIPAA compliance?

HIPAA doesn't mandate the way documents are signed, so an electronic signature doesn't conflict with the law, but it doesn't constitute compliance on its own. HIPAA governs the use and transmission of PHI, which may or may not be contained in e-signed documents. When considering e-signature for HIPAA covered documents, there are specific features to look for to support HIPAA compliance efforts. Healthcare organizations are ultimately responsible for implementing technologies, policies and procedures to ensure that these solutions are deployed in a way that is secure and protects PHI.

Modern e-signature solutions that are interoperable with Electronic Health Records (EHRs) make it easy for patients to electronically sign forms on a device, in a medical office or inpatient at a facility. Electronic signatures have many layers of security and authentication built into them, ensuring information remains private and secure.

Unlike wet signatures, e-signatures include an electronic record that serves as an audit trail and proof of the transaction. The audit trail details the actions taken with the document, including a record of when it was opened, viewed and signed. DocuSign eSignature offers a certificate of completion that includes specific details about each signer on the document, including the consumer disclosure indicating the signer agreed to use e-signature, the signature image, key event timestamps and the signer's IP address and other identifying information.

Once the signing process is complete, all documents are digitally sealed using Public Key Infrastructure (PKI), an industry-standard technology. This seal indicates the electronic signature is valid and that the document hasn't been tampered with or altered since the date of signing.

## What level of authentication is required to maintain compliance under HIPAA?

The level of authentication that's right for your organization depends on your business practices and needs. E-signature technology offers multiple options for verifying a signer's identity before they can access the document and sign, including:

**Email address**
Signers enter their own email address, which is compared to the email address used in the invitation

**Access code**
The sender supplies a one-time passcode that signers must enter

**Phone call**
Signers must call a phone number and enter their name and access code

**SMS**
Signers must enter a one-time passcode sent via SMS text message

**Knowledge-based**
Signers are asked questions about information, such as past addresses or vehicles owned

**ID verification**
Signers are verified using their government-issued photo IDs or European eID schemes

For situations where additional levels of signature validity are necessary, some providers offer two additional levels of e-signature that comply with the EU's eIDAS requirements:

**Advanced**
Requires identity verification. Singatures must be uniquely linked to, and capable of identifying the signer.

**Qualified**
Requires face-to-face identity verification. The face-to-face identification can be live, in-person or via an audio/video connection. A QES is unique in that it's considered legally equivalent to a handwritten signature in the EU.

## What is a Business Associate and what is a Business Associate Agreement?

A Business Associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate.

DocuSign is a Business Associate for HIPAA purposes when a healthcare provider uses DocuSign eSignature for documents that contain PHI. DocuSign doesn't have access to the PHI, but it may hold PHI in encrypted form on its servers.

A Business Associate Agreement (BAA) is a contract between a healthcare provider, health plan or other HIPAA-covered entity and a vendor. The vendor is considered a business associate in cases where, as part of the vendor's services, electronic PHI passes through their systems. A signed BAA must be completed by the vendor prior to providing services.

DocuSign has entered into agreements with numerous HIPAA-covered entities.

## Are electronic signatures on medical forms legally admissible in court?

Electronic signatures are legally enforceable in the United States. There are two primary Acts that establish this legality of electronic signatures: the US Electronic Signatures in Global and National Commerce Act (ESIGN, 2000) and the Uniform Electronic Transactions Act (UETA, 1999), which has been adopted by most state legislatures. Both ESIGN and UETA establish that electronic records and signatures carry the same weight and legal effect as traditional paper documents and handwritten signatures. The ESIGN Act states, "A document or signature cannot be denied legal effect or enforceability solely because it is in electronic form."

## Can I connect e-signature into my existing EHR system?

Yes, there are a variety of technologies that make it possible to send patient forms from within an Electronic Health Record (EHR) system and automatically upload electronically signed forms back into the system. By implementing e-signature technology beyond the EHR, organizations can take strategic steps toward improving the patient intake and consent process while managing HIPAA compliance.

**Common HIPAA forms that can be used with e-signature**

New patient intake forms with HIPAA releases

Patient information and policies

Health information release authorization

HIPAA disclosure form

Medical records release form

Notice of privacy practices

Patient rights and responsibilities

# What to look for in an e-signature solution to ensure it supports HIPAA compliance

Not all e-signature solutions are alike. When evaluating potential technologies, it's important to consider how the vendor manages security, data privacy and data storage.

## Information storage and encryption (in transit and at rest)

Appetite for risk security varies from organization to organization and is dependent on both how the industry operates and the corresponding legal and regulatory requirements. But no matter the industry, security is a central concern for all HIPAA-covered entities, and how data is handled is central 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 they encrypt

– What cipher suites 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 they have in place for equipment management and secure media disposal

## Data privacy

As with classification, storage and encryption, it's all about protecting users' data. Does the e-signature solution provider have a privacy program in place, and will it pass the scrutiny necessary to meet the most highly regulated industries, like healthcare? And if you have patients who are California residents, then you need to ensure that the vendor is compliant with the California Consumer Privacy Act (CCPA).

**Considerations:**

– How private information, such as personally identifiable information (PII) and (PHI), is handled

– Whether users are given the option to opt-in or out of receiving information

– How personal data is used

**Ask what data management and privacy practices do they have in place around:**

– Data subject rights

– Data deletion and retention

– Data access

– Data residency

– Subprocessors

– Privacy notices

– Training and awareness

– Governance and accountability

– GDPR and other privacy regulations

DocuSign eSignature customers determine their accounts' retention policies. To learn more about how customers can purge eDocuments, read DocuSign's data management and privacy practices for eSignature.

**Learn more about DocuSign's industry-leading security and privacy practices and view the latest information on system performance and availability on the DocuSign Trust Center.**

## Conclusion

In today's digital and remote world, healthcare organizations need to make it easy for patients to sign intake and consent forms anywhere. With DocuSign eSignature for Certified EHRs, patients can digitally fill out intake paperwork anywhere. Once completed electronically, these documents will be automatically uploaded into the EHR or your document management solution, either with or without a manual review.

**Learn more about the DocuSign Agreement Cloud for Healthcare.**

**About DocuSign**
DocuSign helps organizations connect and automate how they prepare, sign, act on and manage agreements. As part of the DocuSign Agreement Cloud, DocuSign offers eSignature, the world's #1 way to sign electronically on practically any device, from almost anywhere, at any time. Today, over a million customers and more than a billion users in over 180 countries use the DocuSign Agreement Cloud to accelerate the process of doing business and simplify people's lives.

**DocuSign, Inc.**
221 Main Street, Suite 1550
San Francisco, CA 94105

**docusign.com**

**For more information**
sales@docusign.com
+1-877-720-2040