DocuSign®

Whitepaper

DocuSign eSignature for HIPAA Compliance

Using eSignature to transform patient care

Conversations with health plans and providers about digital business processes often begin with a single question: “Is it HIPAA compliant?” With Meaningful Use fueling electronic health record (EHR) adoption, in addition to the need for a secure, auditable solution, it’s no wonder that regulations are top of mind for healthcare and life science professionals. DocuSign is committed to helping our customers meet compliance requirements across all industry practices, and we have already seen providers, health plans, medical device manufacturers and biopharmaceutical companies adopt DocuSign eSignature in a HIPAA-compliant manner.

This overview provides guidance and answers to common questions regarding Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other regulations governing the use of electronic documents and signatures in healthcare and life sciences organizations.

Understanding HIPAA

How does HIPAA impact me?

HIPAA stipulates requirements for managing electronic health care records and transactions. It chiefly concerns the privacy and security of Protected Health Information (PHI).

PHI is typically used for patient identification and treatment. It includes information such as demographic data, medical history, insurance details and lab results.

While technology providers like DocuSign provide solutions that meet HIPAA compliance standards, healthcare organizations are ultimately responsible for implementing policies and procedures to ensure that these solutions are deployed in a compliant way.

How does DocuSign enable HIPAA compliance?

Using DocuSign eSignature increases the reliability, integrity, availability and authenticity of records and signatures. DocuSign's technology allows customers to electronically sign documents in full compliance with ESIGN, UETA and HIPAA. DocuSign is ISO 27001:2013 certified – the highest level of global information security assurance available today – and utilizes a robust architecture that delivers high availability and enables access on nearly any device from almost anywhere. All documents and data are encrypted in transit and at rest. Each DocuSign eSignature transaction includes a fully traceable, tamper-proof audit trail and exportable Certificate of Completion.

What are implications of the HITECH Act and HIPAA Omnibus Rule?

HIPAA compliance requires that PHI is securely transmitted and stored. The HITECH Act, enacted in 2009, extended these protections to include transmission of electronic records and data.

The HIPAA Omnibus Rule, enacted in 2013, put further safeguards on PHI by extending requirements about PHI privacy and security to Business Associates (BAs). This established the need for BA, contractors whose products or services access, create, receive, maintain or transmit PHI, to enter into agreements with HIPAA-covered entities. These Business Associate Agreements (BAAs) are legally binding documents to ensure BA compliance with use and protection of electronic PHI.

Although DocuSign doesn't have access to any PHI, it may hold PHI in encrypted form on its servers, and as such is a BA and has entered into agreements with numerous HIPAA-covered entities.

Protecting PHI

What does DocuSign do with PHI? How do you share it?

DocuSign provides full document encryption to ensure the confidentiality of your data. Documents stored in our ISO 27001-certified and SOC2 audited data centers are encrypted with the AES 256 standard at the application level for customer documents to ensure confidentiality.

It's the responsibility of each HIPAA-covered entity to ensure that PHI stored in encrypted documents is accessed and shared in accordance with HIPAA regulations.

To maintain compliance under HIPAA, what level of authentication do I need to use to make sure the person I am sharing PHI with is actually the person they say they are?

The level of authentication that's right for your organization depends on your business practices and needs.

DocuSign eSignature has several options for verifying signers' identities, including email, SMS, phone, access code, knowledge-based authentication and checking government IDs. For European customers, DocuSign has options to meet both Advanced and Qualified Electronic Signature levels under eIDAS.

This flexibility in matching the level of authentication to transaction risk is a key capability for both legal enforceability and complying with regulations in healthcare.

Learn more about DocuSign authentication options.

Has DocuSign signed HIPAA BAAs with customers to date?

Yes, DocuSign has signed BAAs with healthcare and life sciences customers.

To the extent DocuSign receives or possesses access to PHI, DocuSign complies in full with the privacy and security requirements of HIPAA applicable to DocuSign as a BA of our customer.

DocuSign has BAAs in place with customers who have enterprise accounts and want to be HIPAA compliant. A signed BAA should be in place between DocuSign and the customer prior to transmitting any PHI through DocuSign.

How does DocuSign support HIPAA compliance within its product and platform?

DocuSign helps healthcare and life science customers meet compliance requirements by controlling the signing process and ensuring all information is authenticated and remains both private and secure.

- A complete, court-admissible audit trail accompanies each document
- DocuSign delivers industry-leading data confidentiality with application level AES 256-bit encryption
- A digital checksum (mathematical hash value) validates that documents haven't been tampered with outside of each signing event, to ensure the integrity of customer documents, both in process and completed
- Customers can rely on the authenticity of signers through signature verification and unalterable capture of signing parties' names, emails, public IP addresses, signing events, timestamps, signing location (if provided) and completion status
- DocuSign provides unique features for non-repudiation, including a digital audit trail for every envelope that captures the name, email address, authentication method, public IP address, envelope action and timestamp

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

Using eSignatures in Healthcare and Life Sciences

Are electronic signatures on medical forms legally enforceable?

Medical forms are one type of document that can be signed electronically.

Electronic signatures are legally binding 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."

Not all e-signature solutions are created equal. DocuSign eSignature warrants federal ESIGN and UETA Act compliance and was the first digital transaction company to meet this standard.

Learn more about ESIGN and UETA.

Can I integrate DocuSign into my existing EMR system?

Yes. A leading children's hospital has integrated DocuSign eSignature into their EMR for surgery e-consents. In addition, DocuSign has partnered with SureScripts, a leading healthcare solutions company that purchased Kryptiq, whose patient onboarding product integrates DocuSign into patient intake workflows. Kryptiq's product is integrated into several leading EMR systems with other integrations currently in development.

DocuSign offers an open API that can be used to integrate eSignature into almost any app, website or system. However, most EMRs currently operate as closed-loop systems, so DocuSign can't integrate with them unless they choose to work with us and integrate our technology into their solution. DocuSign works with interoperability as a service provider, Kno2 to help organizations connect systems for secure patient information exchange.

Are electronic signatures HIPAA compliant?

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 signed documents.

DocuSign eSignature's anti-tampering controls ensure the integrity of customer documents, both in process and completed.

How do I update patient information through DocuSign?

It's important to note that DocuSign isn't an Electronic Medical Record (EMR) system – it's not designed to be the source of current information about patients. DocuSign eSignature is used to complete and sign documents, which represent the information available at a given time. Once a document sent via eSignature has been completed and signed, it can't be altered. However, DocuSign can be used to obtain updated information for use in an EMR system. This process can be streamlined by creating templates with set recipient roles, signing tags and information fields for standard forms and documents that you frequently need to complete.

DocuSign doesn't have access to information that customers send through its platform. Once all parties have completed a document, information is considered at rest.

DocuSign employs strong anti-tamper controls to prevent any alteration of your signature or your documents. Our SHA-2 hashing verifies documents have not been modified, and for those who require X.509 digital signatures, our PKI digital certificate technology secures documents and signatures with tamper-evident seals. DocuSign offers DocuSign Express Digital Signatures and also integrates with SAFE BioPharma to provide digital certificates.

Healthcare use cases and customers

Among healthcare providers, what are the most common use cases for electronically completing documents?

DocuSign healthcare customers are providing high-quality, efficient care and spending more time with patients by reducing the time and costs associated with paper-based transactions.

Use cases include:

- Patient onboarding
- Hospital intake forms
- Provider agreements
- Consent forms
- Transition of care documents
- Notice of privacy practices
- Vendor/supplier contracts
- Insurance claims processing
- Drug prescriptions
- Lab reports

What types of healthcare organizations are using DocuSign? Who else is using DocuSign?

Healthcare providers, such as New York-Presbyterian, use DocuSign eSignature to onboard and treat patients faster. Health plans, such as Blue Cross Blue Shield and UnitedHealth Group, have increased efficiencies in agent/broker onboarding and member enrollment.

AstraZeneca · Boehringer Ingelheim · IQVIA · Children's Hospital Los Angeles · McKESSON · Covered California · American HomePatient

---

Today, more than 500,000 customers and hundreds of millions of users in over 180 countries use DocuSign to accelerate the process of doing business and to simplify people's lives.

Globally, 12 of the top 14 pharmaceutical companies and 14 of the top 15 medical device companies use DocuSign.

Learn more about the DocuSign Agreement Cloud for **Healthcare** and **Life Sciences**.

What other HIPAA resources are available?

Understanding HIPAA Privacy for Covered Entities and Business Associates

Summary of the HIPAA Privacy Rule

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

docusign.com

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