docVerify

veriVault™ Verification Platform

HIPAA Compliance

Using Digital Transaction Management to Transform Patient Care

When it comes to transforming and modernizing any aspect of patient care processes, everybody wants to know if it complies with HIPAA. DocVerify *does*. DocVerify upholds a commitment to HIPAA compliancy to customers in the medical and pharmaceutical communities. Read on to learn more about what DocVerify can do for you.

What is the relationship between something like DocVerify and HIPAA?

Each healthcare practice that must meet HIPAA compliancy typically has a set of policies and procedures in place for obtaining signatures and transactions. DocVerify, an electronic signature and transaction product, helps this process move along more quickly and with more accuracy. In the United States, an e-signature is just as legally binding as a handwritten signature according to the U.S. Electronic Signatures in Global and National Commerce Act (ESIGN), which went into effect in 2000, and the Uniform Electronic Transactions Act (UETA), which went into effect in 1999. DocVerify meets the standards set forth by both ESIGN and UETA.

How is DocVerify HIPAA compliant?

Because DocVerify was designed to help your business comply with ESIGN, UETA, and HIPAA, it contains features that offer heightened integrity and security:

- fully traceable audit trail, admissible in court
- anti-tampering controls to ensure document integrity in process and in completion
- the highest levels of security
- data confidentiality with application level AES-256 bit encryption
- various industry-leading options for authentication of signing events
- reliability and availability with 99.99% real-time, secure data application and uptime, and you can count on DocVerify

While healthcare practices are still responsible for putting strategies in place for achieving HIPPA compliancy, DocVerify makes achieving compliancy easier, more accurate, and more reliable.

docVerify

veriVault™ Verification Platform

HIPAA Compliance

What are the most common uses for using DocVerify in the healthcare industry?

Customers use DocVerify to complete and sign documents, which replaces common paper transactions, including:

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

When you use an e-signature solution like DocVerify, you're spending less time and less money on paper-based transactions and putting more time and energy into providing quality patient care.

Can a document be altered once submitted through DocVerify?

No. DocVerify's proprietary patent pending 7 layers of security protects every document, and once a document has been completed and signed with DocVerify, it cannot be altered—the product was designed this way in order to provide the highest quality in security, accuracy, and integrity as per HIPPA standards. In fact, the DocVerify product contains anti-tamper controls like the SHA-256 or SHA-512 hashing, PKI hashing, and PKI digital certificate technology, which guarantee that documents have not been modified by providing verifications, tamper watermarking technologies, and tamper-evident seals.

Does DocVerify have access to any PHI?

PHI, or personal health information, includes:

- patient identification
- treatments
- demographic facts
- medical history
- insurance details

Start Streamlining Your Workflow Today. Visit DocVerify.com.

docVerify

veriVault™ Verification Platform

HIPAA Compliance

DocVerify does not have access to any PHI; however, there may be some encrypted form of PHI on its servers, so DocVerify has entered in agreements as a Business Associate (BA). The need for BAs was established under the 2013 HIPAA Omnibus Rule: any contractor whose product or service touches PHI in any way must enter agreements with HIPAA-covered entities. These legally binding agreements, known as BAAs (business associate agreements), make certain that BAs are in compliance with the use and protection of PHI delivered electronically.

What level of authentication do I need to use to make sure the person I am sharing PHI with is legitimate?

DocVerify offers a range of choices when it comes to authentication levels, so that you can choose the level of authentication that best fits the needs of your healthcare practice. Options include:

- SMS authentication
- biometric voice prints
- knowledge-based authentication

How does DocVerify protect PHI?

DocVerify put its full-document encryption in place to make sure that private, confidential data stays private and confidential. Only you and those who have your authorization can access your documents—DocVerify employees cannot view any encrypted documents or data, don't have those permissions and thus don't have that kind of access.

Additionally, DocVerify has BAAs in place with customers who require HIPAA compliancy; a signed BAA between DocVerify and the customer should be on file and documented prior to submitting PHI through the DocVerify product. Healthcare practices maintain the responsibility of ensuring that PHI stored in encrypted documents is accessed and shared only in line with HIPAA regulations.

Where can I learn more?

Visit www.docverify.com for more information