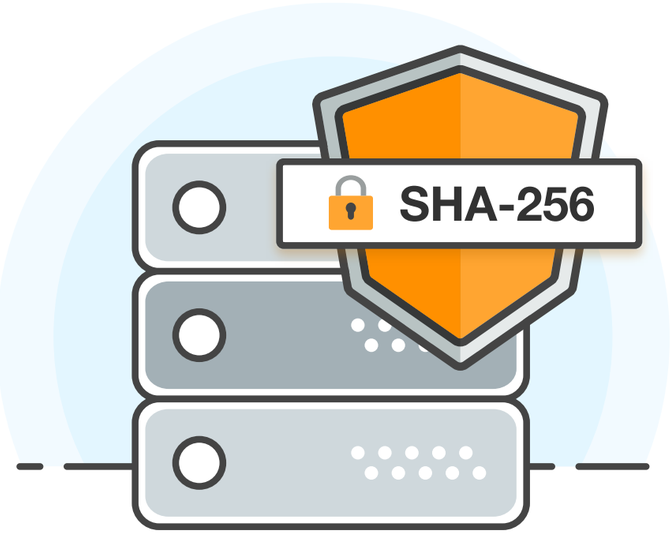
pdfFiller

Learn How pdfFiller Securely Encrypts Data and Keeps Stored Documents Protected

a publication of **pdfFiller**

Data Encryption & Storage

pdfFiller encrypts user communications with the NSA developed SHA-256 encryption algorithm which is used as a security standard in the medical and banking industries to protect sensitive data. All stored documents are housed at Amazon Web Services' secure hosting facilities.

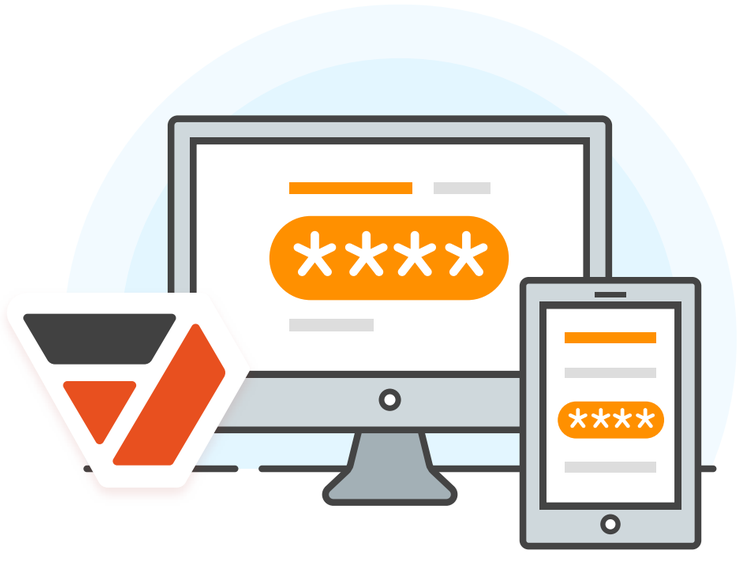


Compliances

pdfFiller complies with PCI DSS the very same digital transaction standard which certifies PayPal and Stripe. For the protection and secure storage of medical documentation, pdfFiller stands alongside other American health care providers such as Blue Cross Blue Shield and Kaiser permanente as 100% HIPAA compliant. pdfFiller is in the process of verifying and achieving the SOC 2 compliance's five "trust service principles”.

Two-factor Authentication

Enable two-factor authentication for eSignature requests by requiring recipient identity verification via code, social media or webcam. Documents containing sensitive information can also be placed into a protected folder requiring an additional password to access.



Signature Certificate & Digital Audit Trail

SendToSign's Signature Certificate maintains the integrity of the signature process by summarizing who signed a document as well as when it was signed and returned. For every document accessed, users can view a Digital Audit Trail that details specific identifying information.

pdfFiller actively integrates the most modern security systems into it's own processes. However, even with the knowledge of these systems in place, businesses and users alike often demand additional layers of certainty to ensure the integrity of their data.

The protection of stored data and transmitted data make up pdfFiller's foundation for digital security. User documents are housed at remote locations, stored on Amazon's Simple Storage Service (S3) data centers, which protects them against any potential data loss. Securing the transmission of data with a 256-bit encryption algorithm means that the communication of data between users, or a user and server, is impossible to intercept and decipher by an outside party.

When a user requests an electronic signature with pdfFiller's eSignature solution SendToSign, they're presented with further authentication options. Document authors can require their recipients to verify via webcam or by sending a unique passcode by phone number that will be required for accessing the document. pdfFiller also offers users an option to place documents into a protected folder that requires an additional password for access. Using these forms of two-factor authentication enables users to go one step further with their document security as well as with documents sent to outside contacts.

pdfFiller is certified compliant with PCI DSS to ensure the security of digital transactions as well as HIPAA for the secure transmission and storage of medical information. Whether a customer's data is in transit or routed through third party service providers, their documents and data are protected and accounted for at all times.

Keeping The Cloud Safe

“64% of Americans cave in to digital extortion”

Symantec Corporation

“64 percent of Americans cave in to digital extortion” - Symantec Corporation

Verizon’s 2017 Data Breach report revealed that healthcare is the second most targeted industry when it comes to ransomware attacks; the only industry more targeted than healthcare is financial services. Additionally, this report found that in 2017, 72% of malware attacks on the healthcare industry were specifically ransomware attacks.

Vulnerabilities in cloud infrastructure provide cyber criminals with openings that can be exploited in order to gain access to private databases. Tens of thousands of databases were hacked and held for ransom in 2016 after users left outdated versions exposed, without authentication turned on.

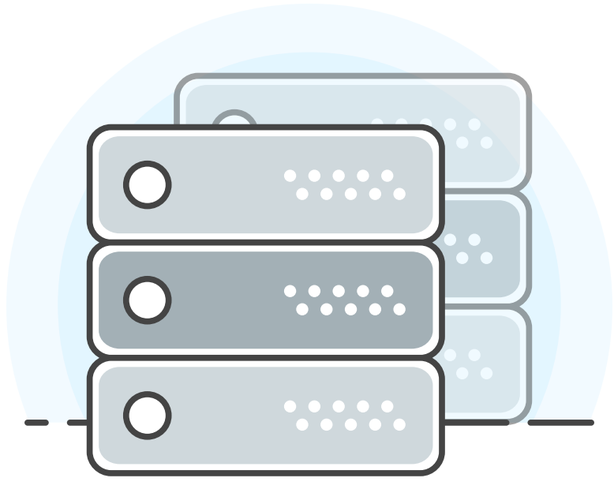
pdfFiller uses the Secure Hash Algorithm at 256 bits (SHA-256) to encrypt user data at every level. SHA was developed by the United States National Security Agency (NSA) and is required for use in certain U.S. Government applications, including use within other cryptographic algorithms and protocols for the protection of sensitive unclassified information.

While encrypting data that is transmitted from one end to another protects users from having their data intercepted, safe-guarding stored data is an equally important measure. pdfFiller documents are stored on Amazon’s Simple Storage Service (S3) which utilizes three different forms of encryption coupled with machine learning to automatically discover, classify and protect sensitive data hosted by Amazon Web Services (AWS). S3 satisfies compliance requirements for virtually every regulatory agency around the globe.

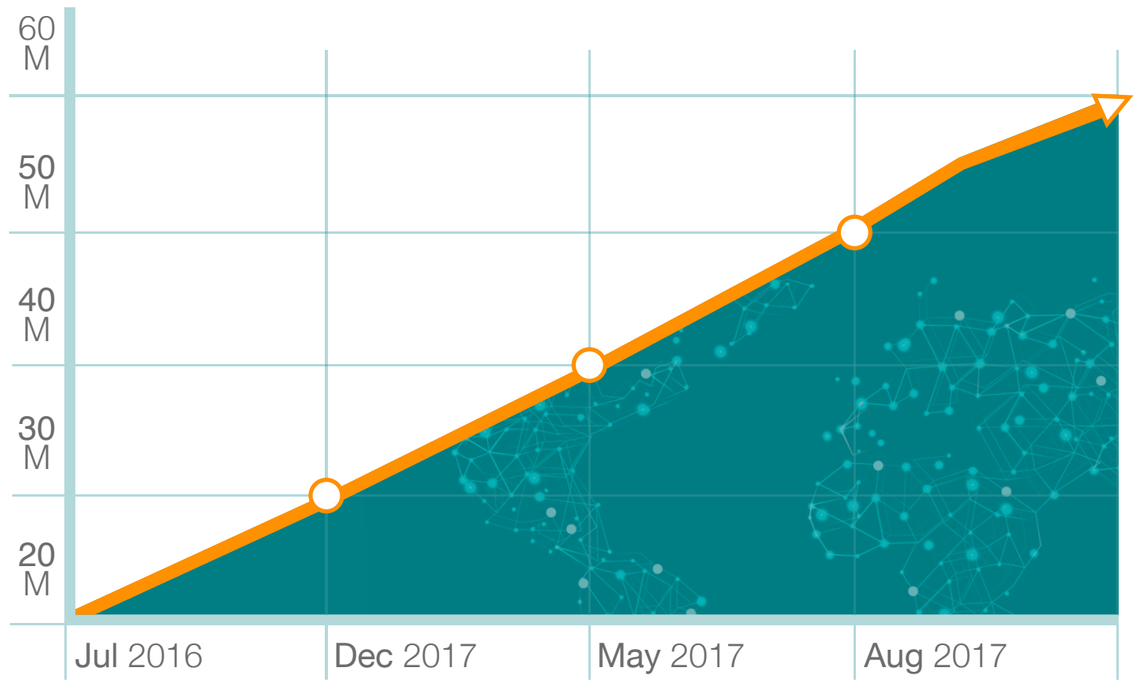
“pdfFiller acknowledges its customers’ need for security as top priority.”

Eugene Gorelik, Director of Engineering

“pdfFiller acknowledges its customers’ need for security as top priority.” said Eugene Gorelik, Director of Engineering. “Early on, when the topic of data storage arose, we knew we would need a service that could not only meet our expectations but one that could scale with the rate of growth we were predicting. Data needed to be kept safe, but it had to be easily accessible as well. We’re proud to be able to deliver top-notch security combined with ease-of-use so that when users need to access documents stored on pdfFiller cloud databases, they’re only a few clicks away from being able to do so at any time, from any place.”



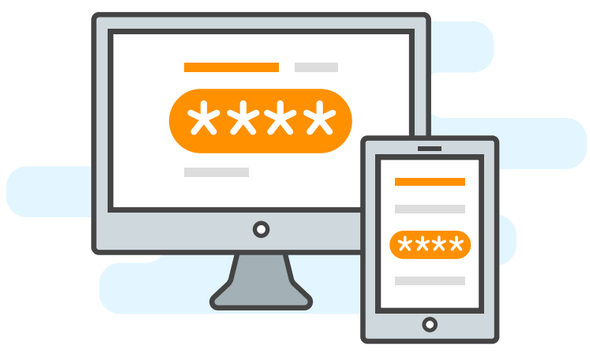
Data storage increased by 3-4x over the past 12 months



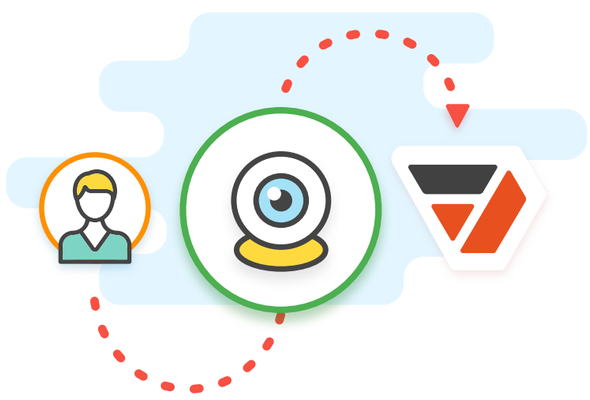
Why Signatures Are So Sensitive

A personal signature, like a fingerprint or iris scan, is a form of personal identification that grants approval for services and transactions to be authorized and carried out on a person's behalf. pdfFiller's eSignature solution (SendToSign) offers users various authentication and security features for identity verification as well as absolute adherence to the eSign Act of 2000. SendToSign maintains high levels of security without sacrificing signer convenience.

Authenticate via social media



2-factor code authentication via text message



Webcam identity verification

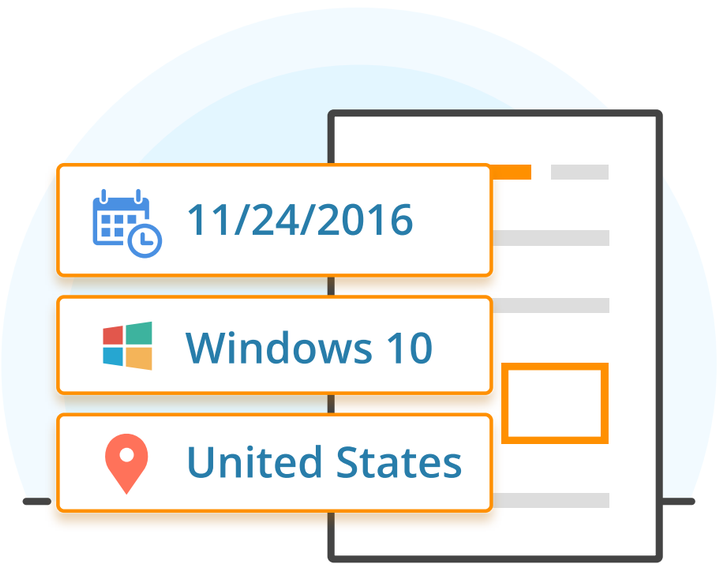
However, an electronic signature is not the same as a digital signature. An electronic signature is any sound, symbol or process that is electronically associated with a contract or record that is adopted by the signer, indicating their intent to sign. Electronic signatures can be verbal authorizations, electronically signed authorizations, or even the simple click of a checkbox. Digital signatures embed a unique digital "fingerprint" into documents and the signer is required to possess a certificate-based digital ID (a digital certificate) in order to link the signer and document.

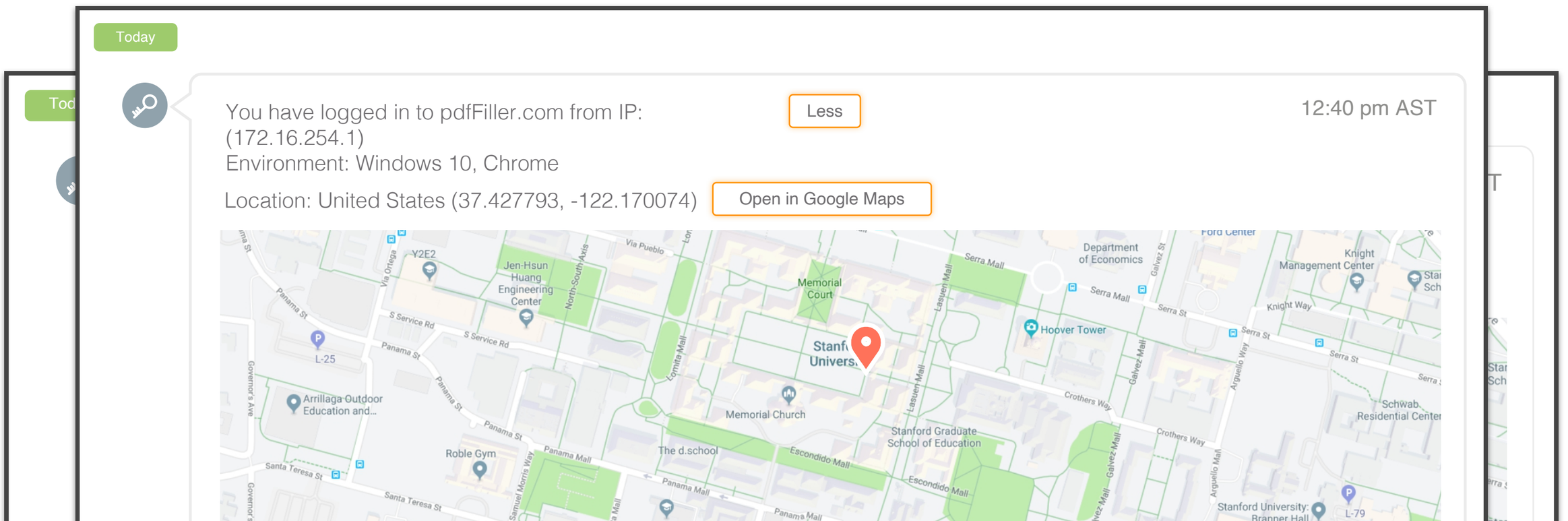
pdfFiller's Signature Certificate

For users that require a record of signatures they receive through SendToSign, pdfFiller offers the Certificate feature, which contains a detailed report about who signed the document, when it was signed and returned, and important information about the document itself. The Certificate is available to download from the SendToSign History folder, and the owner of the document should retain a copy of the Certificate for their record-keeping. Should the signature be contested in the future, the Certificate serves as an "associated record" that maintains the details of the electronic signature process.

Digital Audit Trail

Every document generated, edited, moved or shared has a unique digital audit trail that records specific identifying information such as IP address, geo coordinates, browser, OS information and time stamp. These identifiers make certain that the chain of custody is, and can never be tampered with or altered. pdfFiller's audit trail ensures that each document is technically and legally sound.





HIPAA Compliant

pdfFiller complies with the Health Insurance Portability and Accountability Act's hosting standards thanks to AWS's rigorous adherence to the specific administrative, physical and technical safeguards that HIPAA requires.

Physical safeguards include limited facility access and control with authorized access in place. Technical safeguards require access to control which allow only authorized personnel to access electronic protected health information (ePHI). Network, or transmission, network security is the last technical safeguard required of HIPAA compliant hosts to protect against unauthorized public access of ePHI.

PCI Compliant

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI DSS specifies twelve requirements for compliance, organized into six logically related groups called "control objectives" which pdfFiller complies with for every monetary transaction a customer makes.

SOC 2 Compliance

System and Organization Controls type 2 (SOC 2) defines criteria for managing customer data based on five “trust service principles”—security, availability, processing integrity, confidentiality and privacy. SOC 2 is an auditing procedure that ensures your service providers securely manage your data to protect the interests of your organization and the privacy of its clients.

While SOC 2 compliance isn’t a requirement for SaaS and cloud computing vendors, its role in securing your data cannot be overstated. pdfFiller is undergoing audits to ensure the requirements for each of the five trust principles are met.

Meeting the Demand & Defying Expectation

Any SaaS platform that operates in the protection of private information and digital transactions can be measured by the integrity of the systems which secure that data. Encrypting data communications, transactions as well as housing documents at secure storage facilities that meet federal compliance standards make up the foundation of pdfFiller’s security apparatus.

Additional security features such as two-factor authentication for eSignature identity verification and password-protected folders offer enhanced safeguards for sensitive data. An active digital audit trail as well as the availability of eSignature certification maintains document and eSignature integrity in the form of a digital fingerprint.

For the cost of a single USPS priority mail express parcel sent once per month, an annual pdfFiller subscription serves and secures all user data on a level that fulfills government agency requirements.