DocuRep

Data Security

DocuRep is a cloud-hosted application and utilizes a scalable on-demand infrastructure to accommodate any amount of growth or activity. DocuRep operates its cloud servers with one of the largest, most secure cloud providers in the world.

This secure global infrastructure provides a trustworthy foundation for enterprise systems and applications. Our cloud partner establishes high standards for information security within the cloud and has a comprehensive and holistic set of control objectives, ranging from physical security through software security. This secure global infrastructure is subject to regular third-party compliance audits. Furthermore, our cloud partner has an ISO 27001 certification and complies with a broad, comprehensive security standard and follows best practices in maintaining a secure environment.

All electronic communication between users and the DocuRep system occurs through a high-grade 256-bit SSL encryption, which is the industry standard for secure web transactions and e-commerce. DocuRep employs SSAE 16 Type 2 SOC 1 certified Tier-1 controls with greater than a 99.95 guarantee uptime to host our servers. The SSAE 16 Type 2 SOC 1 examination process regularly and independently evaluates our host's ISO-27001-based security policies and procedures.

In addition to industry certifications, our cloud services partner provides the following enterprise-level security standards:

Physical Security:

- Datacenters in nondescript facilities
- Physical access strictly controlled
- Must pass two-factor authentication at least twice for floor access
- Physical access logged and audited

Hardware, Software Network:

- Systematic change management
- Phased updates deployment
- Safe storage decommission
- Automated monitoring and self-audit
- Advanced network protection

Secure Credit Card Transactions -PCI-DSS Level 1

We maintain the highest standards for credit card transactions. Our cloud partner is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS).

DocuRep runs its application on a PCI - compliant technology infrastructure for processing and transmitting credit card information in the cloud.

In February 2013, the PCI Security Standards Council released PCI – DSS Cloud Computing Guidelines. These guidelines provide customers who are managing a cardholder data environment with considerations for maintaining PCI – DSS controls in the cloud. Our cloud partner has incorporated the PCI – DSS Cloud Computing Guidelines into the PCI Compliance Package for customers.

This PCI Compliance Package Includes the PCI Attestation of Compliance, which shows that our cloud partner has been successfully validated against standards applicable to a Level 1 service provider under PCI – DSS. In addition to hosting in one of the most secure cloud environments in the world, DocuRep uses, a leading payment gateway for processing its customers' payments.

DocuRep's payment gateway is also a validated Level 1 PCI DSS Compliant Service Provider and is listed on Visa's Global Compliant Provider List and MasterCard's Site Data Protection List.

DocuRep never stores raw magnetic stripe, card validation code (CAV2, CID, CVC2, CVV2), or PIN block data. Storage of this data is prohibited by the Payment Card Industry Data Security Standard (PCI DSS).
DocuRep meets the highest standards in PCI-DSS compliance, thereby resulting in a very secure environment.

Privacy Protection

DocuRep never requests or accepts Social Security numbers from anyone. In fact, we ask everyone to remove or black out Social Security numbers from all uploaded documents.

If a Social Security number is visible on an uploaded document, DocuRep's policy is to destroy the document and ask for a new one from the user which contains **no** visible Social Security number.
DocuRep also never requests or accepts Driver's License numbers.

DocuRep never has and never will sell, rent or make our user's personal information available to third party organizations for any purposes not related to the functioning of the DocuRep system.

Passwords:

DocuRep does not grant its employees access to passwords of any DocuRep user, whether it be a vendor or healthcare user. If you forget your password, you must request a password reset.

Passwords are required to be changed every 90 days.

Health care system users and vendors will have complete privacy of their account information, with the exception of their public profile information.

NOTE: For more information, please see DocuRep's "Privacy Policy" and "Terms of Use" documents.