+WD +WoundDesk

Security at +WoundDesk

WHITE PAPER, MARCH 2016

wounddesk.com

At +WoundDesk, the security of your data is our highest priority.

We value your online security as much as you do. And for good reason: every healthcare provider using our service expects their data to be secure and confidential. We understand how important the responsibility of safe-guarding this data is to our customers, their patients and work to maintain that trust.

If you have additional questions regarding se-curity, we are happy to answer them. Please write to us and we will respond as quickly as we can.

— Andreas Lorenz, Lead technology @ digitalMedLab

Trust and transparency

Trust is the foundation of our relationship with You. We value the confidence you've put in us and take the responsibility of protecting your information seriously. To be worthy of your trust, we built and will continue to grow +WoundDesk with an emphasis on security, compliance, and privacy.

As transparency is one of the principles on which our company is built, we aim to be as clear and open as we can about the way we handle security. Should a security breach occur, we will promptly notify our users via our blog, Twitter and/or email of the nature and extent of the breach, and take steps to minimize any damage.

Privacy policy

You own your data, and whether it's your personal or patient information, we're committed to keeping it private. Our privacy policy clearly describes how we collect, use, protect and handle your information when you use our websites, software, and service.

For more information on our commitment to providing secure services, please see our Privacy Policy, and Terms of Service.

Protect and control

+WoundDesk is designed with a secure, distributed infrastructure with multiple layers of protection. We work behind the scenes to protect your data and empower account administrators with tools that provide control and visibility. Our robust information security management framework is designed to assess risks and build a culture of security at +WoundDesk.

Data Center Security

- ISO 27001 certified data hosting in Switzerland
- Round-the-clock video surveillance
- Biometric scanning for controlled data center access
- 24x7 onsite staff provides additional protection against unauthorized entry
- Redundant internet connectivity

Data Security

Customer Data is stored redundantly at multiple locations in our hosting provider's data centers to ensure availability. We have well-tested backup and restoration procedures, with a maximum retention period of 90 days, which allow recovery from a major disaster. Customer Data is automatically backed up off site. The Operations team is alerted in case of a failure with this system.

We do not retroactively remove repositories from backups when deleted by the user, as we may need to restore the repository for the user if it was removed accidentally.

Additionally account administrators of any +WoundDesk services plan can export team and patient Data to backup locally.

All passwords stored in our databases are salted and hashed using an industry standard hash function.

Application Level Security

+WoundDesk supports SSL encryption throughout the application. SSL is a bank grade security protocol that allows your information to be transmitted securely.

+WoundDesk account passwords are hashed. Our own staff can't even view them. If you lose your password, it can't be retrieved—it must be reset.

Login pages have brute force protection with rate limiting.

We perform regular automated and manual vulnerability scans of our applications using accredited industry standard tools to identify and patch potential security vulnerabilities and bugs.

+WoundDesk maintains an extensive, centralized logging environment in its production environment which contains information pertaining to security, monitoring, availability, access, and other metrics about the +WoundDesk services. When problems are detected, our team is notified immediately and the issues are investigated.

Mobile App Security

We have implemented a double layer of security by using an unique AppKey per organization and your Username and Password.

Sensitive data is always transmitted via SSL and no customer data is stored in the mobile app. Additionally all cached data is deleted when you logout of +WoundDesk.

Sessions are, on the mobile app and the web-based administration, limited to 20 minutes of inactivity before they are terminated, reducing the risk that a users unattended mobile phone or computer provides unauthorised access to their data.

Credit card safety

When you sign up for a paid account on +WoundDesk, we don't store and don't handle anysestive credit card data on our servers (PCI compliant).

For the payment process we work together with our partner Stripe. Stripe exceeds the most stringent industry standards for security. Click here to learn more about the technical details of Stripe's secure infrastructure.

Internal Protocol & Education

All employees are required to read and sign our comprehensive information security policy covering the security, availability, and confidentiality of the +WoundDesk services.

All of our employees and contract personnel are bound to our policies regarding customer data and we treat these issues as matters of the highest importance within our company.

Should an account owner ever reach out to our support team for assistance, a support member can shadow an account. Otherwise, employee access to user accounts on our end is limited.

All new employees are given security guidelines for using social media, including information about social engineering.

Protecting Ourselves Against You

Yes, you heard that correctly. We can do everything possible for security, but if your computer gets compromised and someone gets into your +WoundDesk account, that's not good for either of us.

We monitor and will automatically suspend accounts for signs of irregular or suspicious login activity.

In addition to our scalable algorithms, we employ another layer of human reviewers, who monitor for anomalous account activity.

Certain changes to your account, such as your password, trigger email notifications to the account holder.

Protection by Yourself

In addition to the work we do at the infrastructure level, we provide account administrators of paid versions of the +WoundDesk services with additional tools to enable their own users to protect their patient data.

We also make it easy for administrators to remotely terminate all connections and sign out all devices authenticated to the +WoundDesk services at any time, on-demand.

Detailed access logs are also available both to users and administrators of paid teams. We log every time an account signs in, noting the type of device used and the IP address of the connection. Something doesn't look right? Contact us.

The application enforces a strong password quality requirement on all users ensuring that passwords will be between 8 and 15 characters in length and must contain at least one upper case, one lower case and one numeric character.

We enforce screens lockouts and the usage of full disk encryption for company laptops.

Custom integration plan

We're extremely concerned and active about security, but we're aware that many institutions are not allowed or comfortable hosting patient data outside their firewall. For these institutions we offer a custom integration plan, a version of +WoundDesk that can be installed to a server within the institution's network.

Need to report a security vulnerability?

If you believe you have found a security vulnerability on +WoundDesk, please let us know right away. We will investigate all reports and do our best to quickly fix valid issues.

We hope you enjoyed this white paper. Please share your thoughts with us @digitalMedLab using #security, or find us on facebook.

Summary

digitalMedLab takes the privacy, security and protection of your data very seriously. We have built our services, including +WoundDesk, around this priority. Our security policies and controls align with industry standards, and we review them regularly to ensure continued compliance.

Healthcare providers, Physicians and Nurses can confidently use the +WoundDesk services to assess and document chronic wounds, knowing that their data is protected by the architecture and policies outlined in this document.

For more information about +WoundDesk go to: https://wounddesk.com

For a copy of this white paper as PDF, visit: https://wounddesk.com/security

SHARE

About digitalMedLab

digitalMedLab is transforming how people, businesses and IT work and collaborate in the cloud era. Its portfolio of GoTo cloud services enable people to work from anywhere with anyone by providing simple-to-use cloud-based collaboration, remote access and IT support solutions for every type of business.

Learn more about our products and services at: **https://digitalmedlab.com**