RevMan Web Security overview

General Data Protection Regulation (GDPR)

RevMan Web complies with the General Data Protection Regulation regarding processing of personal data of people in the European Union.

More information about Cochrane Privacy Policy on https://community.cochrane.org/organizational-info/resources/policies/policies-all-members-and-supporters/cochrane-privacy-policy

RevMan Web requires Cochrane Account to access. See more info about Cochane account on https://help.cochrane.org/kb/article/82-cochrane-account-help/

End-to-End Security

RevMan Web is hosted entirely on Amazon Web Services (AWS), providing end-to-end security and privacy features built in. For additional, more specific details regarding AWS security, please refer to https://aws.amazon.com/security/.

Data Center Security

RevMan Web customer data is hosted by Amazon Web Services (AWS), which is certified SOC 2 Type 2. AWS maintains an impressive list of reports, certifications, and third party assessments to ensure complete and ongoing state-of-the-art data center security.
Our infrastructure is housed in Amazon-controlled data centers in London and Ireland. Data centers themselves are secured with a variety of physical controls to prevent unauthorized access. More information on AWS data centers and their security controls can be found here.

Application Security

Communications are encrypted over 256 bit SSL

Communications are encrypted over 256 bit SSL, which cannot be viewed by a third party and is the same level of encryption used by banks and financial institutions.

Single sign-on (SSO)

Authentication is through Cochrane Account single sign-on using the OpenID Connect protocol.

Multi-tenant SaaS

RevMan Web was designed as a multi-tenant Software-as-a-Service (SaaS), allowing updates instantly available to all users. Separation of customer account data and user permissions are baked in at every level in the software stack.

Granular user permissions

Permission to access reviews is granted via one of the following routes:

- The user has a role that allows them to manage reviews within the unit that owns the review (this applies to reviews owned by organizations). This includes unit leads, organization administrators, and system administrators (limited IT and support staff).
- The user has a role that allows them to access reviews within the review group that owns the review (this applies to Cochrane and Campbell reviews managed via Archie).
- The user has a role on the review (e.g. author). If the review is owned by an individual (rather than an organization), access may in addition require a subscription.

No other users will have access to the review, with the following exception:

- Users that have permission to access published versions of Cochrane reviews may be able to view these versions and export or copy them.

Data encryption at rest

All data for RevMan Web is encrypted at rest.

Monitors ongoing security, performance and availability

Cochrane monitors RevMan Web to reduce any unexpected downtime to the minimum.

Cochrane applies strict security standards and measures throughout the entire organization. Every team member is trained and kept up to date on the latest security protocols.

Vulnerability scanning

Cochrane does automated application vulnerability scans over RevMan Web and applies the relevant security patches as soon as possible to reduce the likelihood of a data breach or malicious attack.

Backups

Daily backups are done automatically and trasferred outside of the AWS datacenter.