



TECH-FACTS RESEARCH MANAGER

Adding value
to data

This checklist contains a system assessment of Research Manager software (hereinafter referred to as RM). RM is a SAAS (Software as a Service) solution and licensed on a subscription base and is centrally hosted in the Netherlands. RM can be accessed via a web browser.

Certification & compliancy

- ResearchManager (TM of Cloud9 Software B.V.) is ISO 27001:2013 and NEN7510 certified by DEKRA. The ISO 27001 and NEN7510 certificate gives customers and relations the assurance that their data and information will be handled with care;
- RM is GCP, 21 CFR PART 11 and GRPR compliant. RM is designed, developed and tested in close collaboration with the industry;
- Security pen-tests are performed on RM. Documentation is available upon request.

Administration

- Every RM licensee has one or more designated (system) administrator(s).

Changes to the data

- RM captures changes made to the data with an extensive audit trail;
- RM audit trail can easily be viewed exported and printed for auditing purposes;
- RM audit trail cannot be changed;
- RM audit trail captures which user changed data on which moment (date time) and the old and new value of the changed data;
- Depending on RM system settings, changes have to be commented by the user;
- RM account activity is extensively logged.

User documentation

- RM operating instructions are available online;

RM Access

- RM access can be used with IE 9, 10, 11. Edge and can be used with Firefox and Chrome;
- Patient Self Service is optimized for multiple browsers;



TECH-FACTS RESEARCH MANAGER

Adding value
to data



Software versioning & updates

- RM has monthly software updates;

Software Access

- RM is protected with an extensive role based access management system with two factor authentication, a combination of username and password and a 6 digit code;
- RM permissions to perform certain operations are assigned to specific roles and can be enforced on application, module, study, site and patient level;
- RM Level of password strength can be enforced by system administrator;
- RM password change policy for a specific period can be enforced by system administrator;
- RM username is unique;

Hardware/software security

- RM servers are located in a secured and certified data centers located in Hengelo (OV) and Enschede. Both in The Netherlands;
- These datacenters are Certified for ISO 9001, 14001 and 27001:2013 and NEN7510;
- Within the secure area of the datacenters there are RM specific secured areas which are only accessible for authorized Cloudg staff;
- These areas are only accessible for authorized Cloudg staff which has been assigned by Cloudg management.

Secure connection

- Internet connection with RM is secured through EV (Extended Validation) TSL certificates from Comodo.

System backup procedure

- RM has a continuous synchronization full back up to a dedicated backup server on a secure location (3 months storage). The backups are encrypted (AES 256);
- RM has a weekly full back up to a dedicated backup server on a secure location (3 months storage). The backups are encrypted (AES 256).
- RM backup restore is tested periodically.



TECH-FACTS RESEARCH MANAGER

Adding value
to data

Data ownership

- All RM data stored on behalf of the customer is solely the property of the customer;
- For every customer a Processing Agreement will be signed.

Data re-use

- All data collected by the RM users is available for export to Excel, Word, pdf or SPSS format.

Platform

- RM is developed in Microsoft ASP.NET framework 4.0, in C#, within Microsoft Entity Framework.

User interface

- RM user interface contains components from Telerik RadControl for ASP.NET AJAX.

Operating system

- Windows Server 2012 R2 and Windows Server 2016.

Database

- SQL Server 2014.

Servers

- HP Proliant DL360.