

Brief Company Summary

- MediCase AB founded 2014
- We are profitable, with a Equity ratio (financial solidity) of 79%.
- Our goal is to provide a professional eCRF at a cost that is manageable also for small and mid-sized investigator-initiated studies
- We fully host the eCRF on our own continuously maintained IT infrastructure, we set up the study and hand over an eCRF that is ready to start using, we provide support, and we give warranties for the system
- Currently around 60 studies are using MediCase eCRF, the majority being investigator-initiated studies but we also have several corporate customers.
- We have studies ranging from tiny single site studies with less than 20 subjects up to studies with several 10's of sites and several thousand subjects. Among the studies there are study sites in many EU/EEA countries, including Germany, Denmark, Sweden, the UK, the Netherlands, France, Spain, Italy, Greece, Finland, Norway, Switzerland, Iceland.
- Customer feedback we receive is particularly positive regarding user friendliness and ease of use, fast turnaround from contract to system being up and running for live use, and a good and relevant set of system features at a manageable cost
- Leadership team, also owners, consists of Computer Engineer, Clinical Data Manager, and M.D/Researcher

Security Summary

- All system access requires personal user account
- System permissions limited based on user account roles
- Username/password and 2-factor authentication (2FA) by means of SMS code, smartphone app, or smartcard
- User is automatically logged out after a period of inactivity
- User logs and audit trail with system generated time-stamps available for traceability/audit of user access and data entry/edits
- Connection between web browser and server is encrypted using HTTP over SSL.
- Server facility has perimeter protection (controlled physical entry access, reinforced walls/doors, etc), fire protection, and is guarded 24/7.
- Data backed up 3 times daily, and weekly to a physically different location. All backups are encrypted. Backup recovery testing performed and documented regularly
- Server runs behind firewall and with regularly updated anti-virus protection
- Documented penetration testing is performed regularly on servers (i.e. a wide range of test are applied regularly to test the systems resistance to intrusion attacks)
- Documented risk analyses reviewed and revised several times per year to identify new/changed potential threats, and as applicable mitigation is implemented
- Every modification to the system is tested and validated through documented System Development Lifecycle (SDLC) process, including following leading industry software security standards such as OWASP, before it is released to users

- Outdated web browser versions that are no longer supported by the browser manufacturer, more specifically do no longer receive bug- and security updates from the browser manufacturer, may be blocked from access the system if we identify the browser poses a security risk
- All MediCase employees and contactors are bound to confidentiality agreement, and to act according to documented IT/physical security policies.

Notes Regarding EU's General Data Protection Regulation (GDPR)

- GDPR is a regulation, i.e. a common legal act of the European Union that is enforceable as law in all member states. GDPR also applies to EEA.
- GDPR regulates the processing, storage and handling of “personal data”, i.e. any data that is attributable to a physical individual, including e.g. security of systems where such data is stored/processed and organizational measure to protect “personal data”. The health-related data collected in a clinical study is one example of such “personal data”.
- MediCase AB complies with GDPR.
- All servers on which MediCase eCRF runs are owned by MediCase AB (i.e. is not a “cloud” storage) and located in the EU (Sweden).
- There is no data processing/storage outside the EU/EEA
- MediCase will only process the client's data according to the eCRF service contract. A Personal Data Processing Agreement (as mandated by GDPR) is included in standard eCRF service contract.