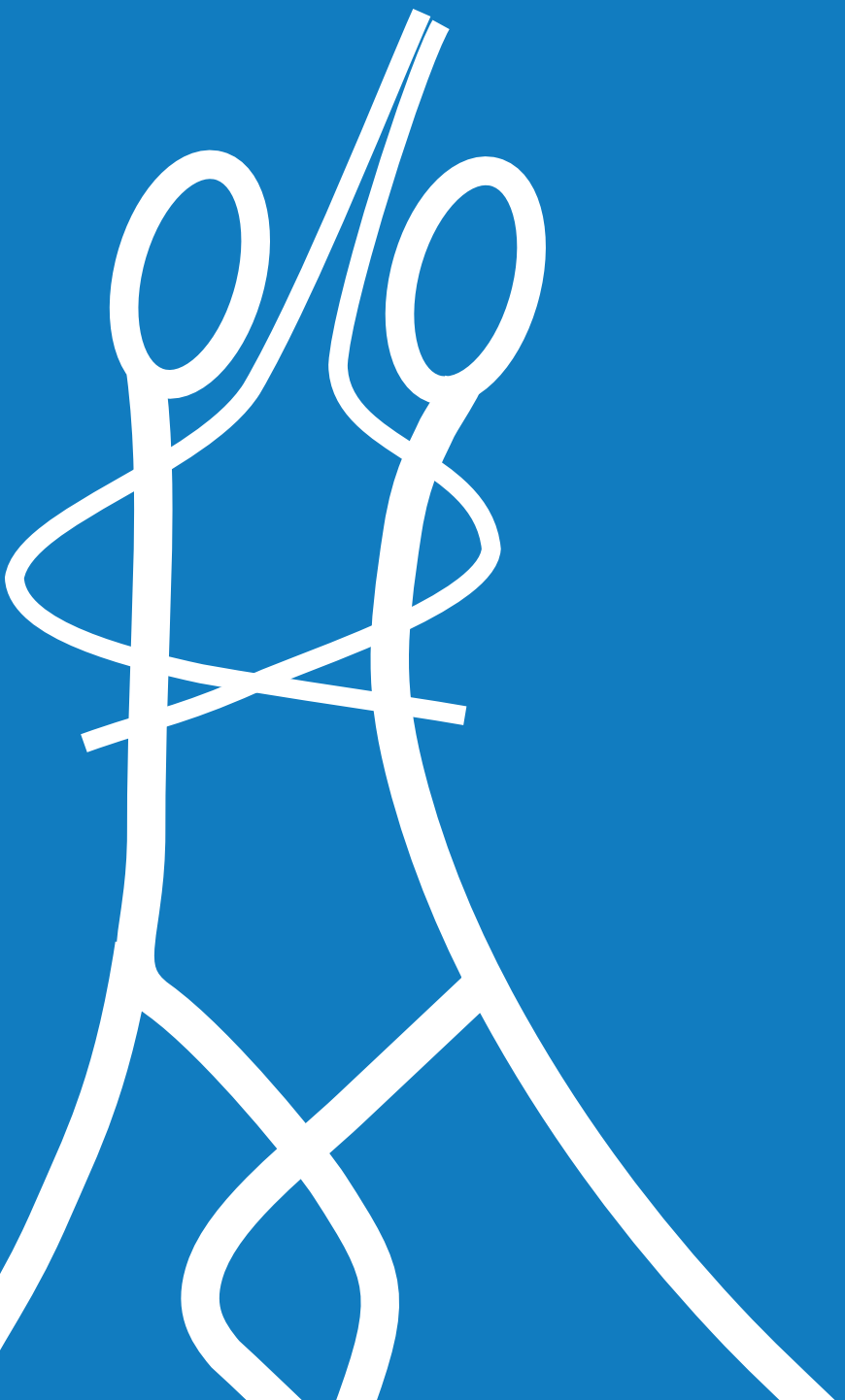
SPINE TANGO Information Security

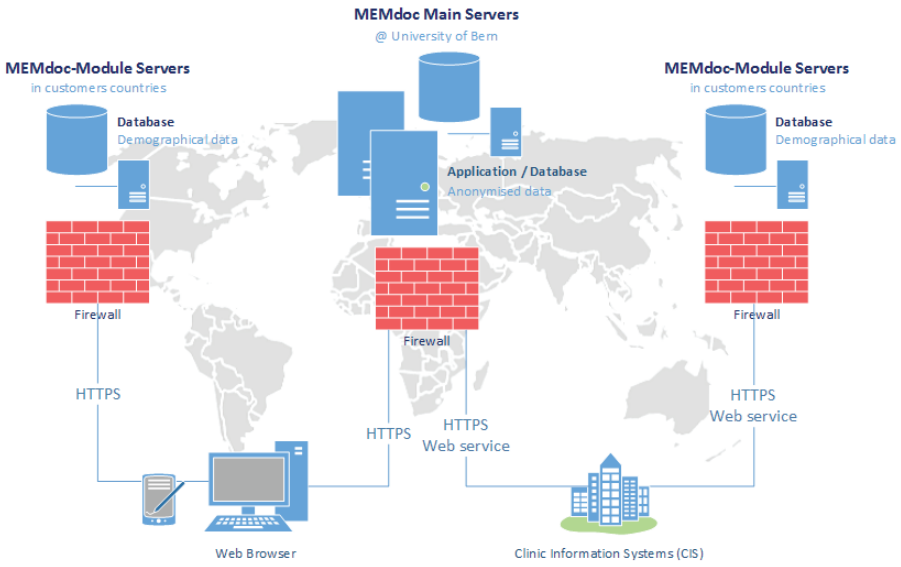


Information Security

IEFM, in its role as a provider of technology resources for collecting, archiving and distributing medical data for research and analysis, is committed to complying with all statutory regulations and guidelines for ensuring the security and privacy of the data submitted through and stored within the MEMdoc portal. Data protection and privacy statutes of the German data protection office of North-Rhine-Westfalia, the French CNIL, the Swiss Federal Data Protection Officer and American HIPAA rules 45 CFR Parts 160, 162 and 164 that govern the privacy and security of the protected health information entered, transmitted and stored, have been passed or are respected within the system through organizational and technological controls.

The model of the MEMdoc and MEMdoc-Module system is designed around the principle of data separation. The MEMdoc central server, housed at the MEM Research Center, Institute for Evaluative Research in Medicine (IEFM) in Bern, Switzerland, hosts the main application and the central database containing all study definitions and clinical study data. The satellite MEMdoc-Module servers are located within the country where the health information is collected and store all personal data about users, institutions and patients. With this technology the MEMdoc-Module database stores ONLY demographic data and the MEMdoc central database stores ONLY de-identified health information. At the core of the system is an innovative architecture in which the web browser of the client is used as a hub to seamlessly segregate and simultaneously integrate the data between the MEMdoc-Module and the MEMdoc central server. This design provides tightly integrated communication between the servers while increasing the security and privacy of both systems. This has been accomplished using a light weight JSON server and incorporation of SSL encryption during all data transfers. Flexible data sharing options have been designed to restrict or expand data access to suit individual needs. Finally, data consistency is controlled through systematic validation of received data and a rollback in case of errors.

MEMdoc and MEMdoc-Module Data Segregation and Web Service



Each module server contains a local MySQL database, an Apache web server and the custom MEMdoc-Module application. This server can sit within the same clinic as the user or in some remote location depending on the needs of the group hosting the module. We suggest a virtual installation on the hardware of IEFM for the first phase of a registry. Alternatively, the registry initiator can name a country and institution of their choice for hosting the module. The physical and network security of this server is provided by the hosting entity. Module hosts can choose to restrict access to the module to users within their local subnet. The module database contains all user and clinic information as well as the basic demographic data of patients. No medical data is stored on the module server.

Users access the system through the URL of their local/national module which then makes its connection to the MEMdoc central server that houses the core MEMdoc application as well as all clinical study definitions. The MEMdoc application recognizes the URL of the connection to determine which MEMdoc-Module to utilize and delivers the appropriate custom module application to the user's web browser. Each time a user requests data the application contacts both the local MEMdoc-Module and MEMdoc central database to seamlessly integrate the data within the client's web browser. Newly entered data is likewise split so that only internal numeric identifiers for the user, patient, clinic, department and module are stored on the MEMdoc central database. All identifiable information about users and patients is only stored on the MEMdoc-Module database. Likewise, all medical data is retrieved from and stored directly to the MEMdoc central server and linked to the module by these internal identifiers. The birth year and gender of each patient are the only pieces of personal information stored on the MEMdoc central data for performing pooled medical statistics.

a. Physical safeguards

The physical and network security of all the MEMdoc servers is maintained by IEFM at the University of Bern. This includes the MEMdoc central (web) server, the MEMdoc database server and the MEMdoc statistics (SAS) server. All servers are physically housed at the MEMcenter in a dedicated, locked, climate controlled and environmentally monitored server room. Physical access to the server room is tightly controlled with access logged and restricted to specific IEFM network personnel. Each server is equipped with redundant internal power supplies and protected against surges and outages. All hardware maintenance is logged and data storage devices are physically destroyed upon disposal. The network is protected by an enterprise level firewall with real-time gateway anti-virus, anti-spyware, anti-spam and intrusion prevention. The firewall only allows web access to the servers from the outside via encrypted connections. Additional access is restricted to connections from within the MEMcenter or through secured VPN connections. Web security is controlled by a DigiCert certified SSL web server certificate with 256-bit encryption on the MEMdoc central server and on each satellite module. Each server is continuously monitored to log all connections and to detect any suspicious activity. In addition to our own IT specialists, the MEMcenter follows all facility security and contingency plans set forth by the University of Bern. The

University regularly audits our security systems, using their proprietary system, to ensure that IEFM security measures consistently meet or exceed industry and regulatory standards.

b. Technical safeguards

Data integrity, patient confidentiality, and security are all integrated into the design of the MEMdoc and MEMdoc-Module systems from the lowest level. The separation of data between the two systems guarantees no individually identifiable health information is available from either system alone. Data can only be joined through the MEMdoc application and even then is only done so within the client's web browser. Access to the system is controlled by username and passwords stored only on the module database using a SHA-256 one-way hash. Both MEMdoc and the module, however, must recognize the user and the module before a user can be securely logged on to both the systems. This is accomplished via SSL encrypted communication through the user's browser using JSON and AJAX. A user ID, signature (signed with RSA private keys), and a session ID are sent from the module server to the user's browser and then transmitted to MEMdoc. The RSA signature ensures that no data is altered during transmission. Once a session is established it is saved on both servers and validated with every transaction. Sessions only remain active during continuous activity and expire shortly upon periods of inactivity. The integrity of the data stored on MEMdoc is controlled by strict testing of all data entry and modification paths as well as periodic extraction and comparison with known sample sets to ensure the consistency, accuracy and reliability of the entire input-storage-extraction path of the data. Audit trails on the MEMdoc database are generated using Oracle's Flashback (http://docs.oracle.com/cd/B28359_01/appdev.111/b28424/adfns_flashback.htm) technology that automatically tracks and archives transactional data changes. Auditing of the module (MySQL) database is accomplished using the binary log of the InnoDB database engine that logs each transaction.

c. Administrative safeguards

Even the most secure IT infrastructure is still as vulnerable as the personnel and policies of the organization. In 2009 IEFM secured the resources of Swiss InfoSec AG (http://www.infosec.ch) to review and formalize its security standards including a risk analysis and risk management appraisal. In 2010 the security and privacy policies of IEFM were approved by the Canton of Berne (Weisung des Regierungsrates über Informationssicherheit und Datenschutz - ISDS). The key points of IEFM's security policy are as follows.

- Associates are made aware as to the sensitivity of the information being handled and the importance of maintaining its integrity.
- All IEFM team members (employees, contract workers and students) are required to sign a confidentiality agreement acknowledging that they understand the importance of maintaining confidentiality and the sanctions for non-compliance.
- The security policy of IEFM is periodically reviewed as a group and available for any IEFM member to read at any time.

- Access to the database and all servers within the organization is following a hierarchical role-concept, and is restricted on a need-to-know basis with strict criteria that establish exactly who has access to specific information.
- Trusted external partners are contractually bound by a similar policy, but are restricted to accessing test data only.
- Upon termination of an employee or trusted partner agreement all physical and system access privileges are revoked.
- IEFM did undergo and is undergoing (unannounced) audits by the Canton (state government) of Berne, to ensure that all of the security and privacy regulations are consistently being followed.