Security in ProMISe version 3

Datum	Naam	Actie	Definitief
08-10-2014	H. J. van der Wijk	Revised	
2014-11-04	R. Brand	Additions (FAQ)	

Advanced Data Management
Medische Statistiek - LUMC
ADM@lumc.nl
www.msbi.nl/promise

Security in ProMISe

This document sketches the security aspects relevant to any project designed and maintained under the ProMISe data management system. Since March 2010 the ProMISe system is NEN 7510 certified by Lloyds. This certificate has been renewed in 2013 according to the new NEN 7510 version of 2011. The approach for this certification has been based on the ISO27001 approach and encompasses a Statement of Applicability and an ISMS. There are several aspects to security and privacy in any internet-based data management system. These aspects relate to the hardware, communication, logistics and storage of information.

Hardware

The ProMISe server is located in the central server room of the Leiden University Medical Center. This area contains also the servers of the Hospital Information System themselves and has professional power, cooling, network and backup systems. The area has restricted access by authorized personnel only with an electronic secure access system.

The hardware of the server has a 4 hour mission critical support with the supplier (Dell) and server configuration and basic operating system software is maintained under a critical-level maintenance contract between the Directorate ICT (DICT) of the hospital (which maintains all hospital servers) and the department of Medical Statistics of the LUMC.

The server has its own software firewall and virus protection as the inner shell of protection. The server is located in a DMZ, a secure zone within the hospital environment, surrounded by a hardware firewall maintained by the DICT. Access to this zone from outside the hospital is allowed only via http and https (SSL encrypted connection). There are very few explicit IP-addresses which can connect to the server via other protocols and they are explicitly and manually entered into the firewall definitions.

Software

The servers dedicated to ProMISe run Windows server, IIS and SQL-server. No other applications than ProMISe related are allowed on these servers. Access to the server itself is restricted to maintenance personnel of the DICT, the system administrator (Watze Hoekstra), the ProMISe scientific programmer (Henk Jan van der Wijk) and the head of the Advanced Data Management section of the Dep't of Medical Statistics, Ronald Brand). All other personnel of ADM has access only through the web-based application interface. Yearly a restore of the entire ProMISe system is practiced, to ensure continuity in case of a calamity.

Each ProMISe project is realized as and restricted to a single database. Each user of the ProMISe project is issued an individual ProMISe username and password. The passwords are required to have a high level of complexity. With these access codes, the user can obtain and modify information in the database via a secure internet connection using SSL (https: protocol). Accounts are blocked when 10 attempts have been made by the same user trying to logon with invalid passwords. Access can be restored only by manual intervention of a project Manager or the central ProMISe administrator. The project manager has to login with an additional security measure: a TAN code send to the mobile phone of the manager. When identifiable (patient) data are stored within a specific project, all users have the

additional security of a TAN code for logon. For each user precise authorizations are maintained in the database and constitute an integral part of the design of such a project. Several levels of authorization can be applied: statistical, individual data reader, individual data modifier, structure modification etc.

All accesses to the project are logged in detail. Username, IP-address and exact date-time stamps are logged for every single action on the system (log on, data retrieval, data save, data reporting, log off). Every modification to every item in the data is logged where previous and current value, user and IP-address is stored together with the exact time of this modification.

Communication

Each project has a Designer and a Manager with extended rights. It is up to the Designer to decide what kind of information is stored in a project. The Designers and Managers are responsible to ensure that all legal requirements are fulfilled with respect to the storage of privacy sensitive information in a database system. From the viewpoint of the ProMISe application, security is maintained by allowing access only over secure encrypted connections (https:), verification of username and password, TAN codes for managers or all users, detailed levels of authorization and extensive logging of actions and modifications. The actual authorization given to a specific individual in the context of a specific project, is the responsibility of the project Designer cq. Manager; the procedure for user management is described in our SOP "user management". All ADM personnel have signed a confidentiality statement.

Storage

All data pertaining to a project are maintained within one SQL Server database. Each database is password protected and the (randomly generated) password is known only to internal software procedures which need access to the database. A fortiori Watze Hoekstra, Henk Jan van der Wijk and Ronald Brand have access to all databases (administrator rights). It is possible to store information that is outside the scope of the Promise Web interface and thus not even accessible via the https: protocol but only internally for a system administrator.

Logistics

ProMISe manages a variety of privacy sensitive projects, including projects with access from outside the EU to data on patients from EU member states. It is the sole responsibility of the individual project management teams to ensure that all data fields in the project comply with legal requirements and the database is properly registered with the relevant authorities.

The ProMISe system is used for Dutch registrations, but also for registrations which are based in other countries. For example a Germany registration, containing only German patients and which are totally maintained from a data center in Germany while still physically residing in Leiden. Also projects, properly registered with the relevant authorities in the Netherlands, are run which contain fully identifiable data on individuals, where these identifiers are encrypted via a TTP. ProMISe also supports all French bone marrow transplantation centers with their scientific data collection while allowing the French authorities statistical access to well defined pieces of information for well described and defined-by-law purposes.

The ProMISe system is NEN 7510 (2011) certified. Each project will have to obtain the additional permissions necessary under Dutch or other applicable law. The actual measures taken are open for inspection in individual cases to relevant authorities. The ProMISe system uses advanced measures to safeguard the privacy of the data and the ProMISe system and databases are maintained at the highest possible level of security which can be expected for a scientific medical research environment and a system which is based intrinsically on Internet access. It is up to the management of the projects themselves to ensure that users comply with safety policies and handle the data confidentially.

References

- SOP User Managament

- Statement of Applicability

Frequently Asked Questions

The list of questions below reflects the usual questions our Department gets about security details, often triggered by requirements put forward by Competent Authorities.

Computer architecture:

1-How the data collection is done: Electronic questionnaire or on line form? Its name?

What is the computer system: One or several servers externalized? Or other (distributed architecture or boarded computer)?

- The data is collected in the Promise Clinical Data Management System. This is a web based system. The server is hosted at the Leiden University Medical Center(LUMC). This is a dedicated server, a Dell R520 with RAID and other redundancy options. The server is hosted in the LUMC computer room where also the other servers like the Hospital Information System servers are located. The level of protection is the same as for the patient data servers.

2-What is the operating system ? its name?

- The server is running on Windows 2012 Server and is fully patched (strict patch policy)

3-The application software is a database. What is its name?

- The data is stored in Microsoft SQL Server 2012

4-Nature of the computer network of the organization dealing with the computer processing: No network (individual isolated)PC? One or several networks on the same site? Several interconnected network (interconnection name?)? one or several externalized networks subcontracted? Wifi technology? Outside Communication? Other?

- The Promise server is connected to a so called DMZ of the LUMC firewall and allows only specific connections such as http and https. A few connection to LUMC internal computer are allowed for management of the server. We only run Microsoft IIS as the webserver technology and the ProMISe application uses CGI. All connections are secure; no other software is allowed to run on the server.

General security:

1-If the data processing requires exchanges with clients, users, a hosting server...Please describe in a few words.

Promise is a Clinical Data Management system. This is a web based system for data entry, validation, reporting and exporting. Safety is of high importance and therefor the department ADM of the LUMC has been certified for NEN 7510 for securing medical information in developing and hosting project for medical research. The certification follows the ISO27001 structure and a Statement of Applicability is available for collaborators.

2-Exchange on Internet (web including portal, file transfer, email). Please detail the encryption methods.

Promise is a web based system that only allows secure ssl/https connections. Patient identifiers like social security numbers, name, address etc are stored using a separate real time encryption system.

3-Describe the security of the room and equipment hosting the system

The server is hosted in the LUMC computer room at the same level as the Hospital Information Systems. This room is only accessible by authorized personnel, has professional power, cooling and network infrastructure.

4-Backup system: type of backup, frequency, security, encryption methods used.

This is at the same level as the HIS servers. LUMC has a central backup facility (robot). Daily backups are being made. Professional procedures are in place to protect the backups, both in safety as in availability (e.g stored on other building than servers)

Intrusion:

1-Protection against intrusion: antivirus? detection of intrusion (IDS), name?, compartment of the network with filters (ex. Firewall, DMZ..)? Treatment confined in network isolated from the others (ex. VLAN)? Other?

The server is hosted in the DMZ of a professional Firewall. The server has professional virus scanner software. The server is constantly monitored, on hardware, Windows and on application event. The server is publically only available for https. Only a few computers have advanced access to the server for administrative purposes.

2-Maintenance of the system: recorded in a journal? Telemaintenance? Physical maintenance in presence of a technician? Maintenance support sent outside are protected (describe)? Maintenance support destroyed are protected (describe)?

Maintenance follows strict hospital policy. No storage devices with information leave the LUMC. For example on removal of a server, disk are professionally destroyed. Access to servers for Dell support only with supervision of LUMC technical support.

Authentification:

1-Caracteristics of the password: Length, validity..

We follow standard requirements of the LUMC: length at least 8 characters, and 3 out of 4 types of characters (uppercase, lowercase, digit, special character) are required

All passwords expire in at most 6 months (can be configured to expire quicker); password is stored encrypted so also sysadmin cannot read them. A once used password cannot be reused

2-distribution: how the password is distributed?

Depends on the configuration. One can demand each password to be distributed via SMS or email or a mixture (depending on the role of the user)

Logging:

1-Access to the application: date and time of connection, Id of the computer, Id of the user, date and time of disconnection, operation performed?

The Promise application maintains a log of all user logins and logoffs. This logs contains the action being performed, the account used, the IP address from which the action took place and of course date and time. A separate log is used for intrusion detection and unlikely or improbable requests

2-Access to the personal data: date and time of connection, Id of the computer, Id of the user, date and time of disconnection, data accessed?

Access to personal data is logged in the same way as access to the application. Loading of (patient) data into memory is logged; actions like reporting or exporting data elements. IP address is always present as well as username; logs of emails or SMS being sent.

3-Logging for :reading, creating, updating, deleting?

The Promise application has a full audit log of all data changes. Both the old and new value, the ip address, the account name are stored. Theoretically the logs allow a full reconstruction of the data up to

any point in time. Deleted records are temporarily stored in a separate table after deletion from production tables to enable quick restore on user mistakes.