UK Inflammatory Bowel Disease Audit
Biologics Audit system and hosted server
Security Details

www.ibdbiologicsaudit.org

For further information contact: biologics.audit@rcplondon.ac.uk

Table of contents

Overview

This document aims to provide information on the security and encryption measures used on the server hosting the Biologics Audit managed by the UK IBD Audit project team.

Note that this document attempts to summarise and give an overview of security measures in place, whilst there may be specific details that have not been mentioned, security procedures designed by Microsoft and industry standard bodies have been followed.

The contracted system developer has also implemented the recommended procedures contained within the NHS "*Securing Web Infrastructure and supporting services Good Practice Guideline*"

Details will be provided on the following:

Physical data centre

Location
Security
Admission control
Climatisation
Electricity
Fire Protection

Operating system

Version
User access
Security
Encryption
Updates and patches
Backups

Database software

Version
User access
Encryption

Application software

Source control
User access
Encryption

Physical data centre

Location

The system developer utilises servers provided by Serverloft, live servers are located in Germany whilst the development server is located in the USA.

Security

The serverloft data centres are protected 24/7 by a security service. Powerful video surveillance of the external facilities and of the entrance areas as well as the internal facilities ensures that no unauthorized persons can enter the technical service area.

Admission Control

Photo recognition systems, biometric palm scanners, and card systems on all inner doors allow only authorized persons to enter the data centres. The security doors with safety glass and steel walls in the entrance and exit areas complete the data centres' comprehensive security concept.

Climatisation

The climatisation of the serverloft data centres follows the principle of N+1 redundancy on full load. All climate modules have a standby compressor and are fed in turns over a redundant climate circuit (a and b). Each circuit consists of a running and a standby pump. Only about 75 % of the available cooling capacity is needed to run the data centres at full load.

Electricity

The permanent power supplies are secured by a sophisticated redundancy concept of multiple power suppliers with several uncrossed conductors. If there is a power outage in spite of this, a UPS (uninterruptible power supply) guarantees that all important components are supplied with power until the emergency power generators take over. For stability reasons, multiple emergency power generators have been installed.

- Capacity: 36 hours at full load
- Refuelable during operation
- Contract enabling refuelling within 180 minutes 24/7

Fire Protection

Two-stage detection systems as well as three-stage fire protection ensure operation even in case of a fire. Early detection systems for smoke and the automatic peripheral sprinkler systems (Marioff Hi-Fog-System) provide timely protection for the critical systems in the data centres and serverloft hardware against fire damage.

Operating System

Version

Windows server 2008

User access

Access to the backend of the server and its associated systems is available to employees of the contracted system developers. Each user has a separate account with a very strong password controlled by password policies. All built in administrator and guest accounts are disabled and service accounts are separate and restricted.

Security

Antivirus, intrusion detection and firewall software is installed on all servers. Firewalls have been restricted to only allow incoming connections from required ports and where possible there ports have been restricted to specific IP addresses as well. File and directory level permissions have been specified for all service accounts. Any unnecessary privileges, services and applications removed.

Encryption

Access to web applications is only available using SSL (443), each application has a valid secure certificate. Further to this the data drives of the server are encrypted using bit locker with the keys only being available to the contracted system developers.

Updates and patches

Anti-virus and intrusion prevention signatures are applied immediately, whilst operating system and server updates and patches are evaluated on our test servers before being applied to the live sites. This is done as soon as practically possible after a new update has been made available.

Backups

Backups are run nightly and are securely stored on the server and 2 off site locations. Each backup is encrypted and transferred either via secure FTP or over our internal VPN, this secures them in transport as well.

Database software

Version

Microsoft SQL server 2008

User access

Access is available only to windows users and service accounts; the SQL user function has not been enabled.

Encryption

The database is encrypted using Transparent Data Encryption this is a technology employed by both Microsoft and Oracle to encrypt database content. TDE offers encryption at a column, table, and tablespace level. TDE solves the problem of protecting data at rest, encrypting databases both on the hard drive and consequently on backup media.

Application software

Source Control

All copies of the source code are kept in 2 locations and are accessible only by users of WestCliff Solutions.

User access

User access is controlled by username and password, the password is controlled by a policy that requires at least 8 characters, at least 1 numeral and at least 1 capital. When a new user is registered they are sent 2 separate emails, 1 containing their username and 1 containing their password.

Every time a new page or section of the application is accessed the user credentials are checked to ensure that a user cannot access data that they do not have permissions for.

Encryption

Password and fields containing sensitive information (e.g. Patient identifiable data) are encrypted within the database using an internal key. This key is contained with the application source code and is only accessible to employees of the contracted system developers.

Overall this means that the data is encrypted 3 times, first at disk level, then at file level and finally the patient identifiable fields are encrypted within the database itself. This provides an extremely secure level of protection that is robust and well within recommended guidelines.