EDGE Security Specifications

EDGE Application Access Controls

Access control is the single most important aspect of data protection, for privacy purposes. If access controls are inadequate all other data protection measures are compromised.

EDGE requires the use of a username and password for access. Users sign on to the application using these credentials. The URL of the sign on page uses SSL/TLS (HTTPS:) security. Any attempts to open under HTTP are forced to HTTPS. This encrypts the session between the client browser and the application within the hosting environment.

Each organization sub-licensing EDGE is responsible for creating and managing the issue of EDGE passwords to their authorized staff in accordance to the licence agreement and to ensure that they are aware of and comply with the data protection regulations.

All site administrators, as per organization policy, will be asked to provide a list or access to a list of all authorized EDGE users from their respective organizations. Any irregularities (e.g., non-registered email domains, generic email accounts) are flagged for follow-up and if required account suspension will be provisioned by site administrators.

EDGE User Account Security

To access the EDGE System, each EDGE user is required to enter the username and password that are automatically generated from the EDGE System upon completion of registration requirements. Once users are created they need to validate themselves via a link before they can use the system. A list of all authenticated users is maintained in EDGE. As per the executed sub-license agreement, each licensing organization retains the responsibility for managing its list of authorized users and ensuring that only such users access EDGE.

EDGE passwords must be at least eight characters long and must include uppercase characters (A-Z), lowercase characters (a-z) and numbers (1 -9) or symbols. Passwords are encrypted. The password expiration policy is set at 180 days by default; passwords must be renewed at least that often. Site administrators can shorten this period to 30, 60, or 90 days, or lengthen it to 360 days.

User access roles include “read only” and “read/write”. All EDGE users have read access to the research projects for which they are authorized; only a subset have read/write access. On a project-by-project basis there is a ‘manager’ who can manipulate the project record and a ‘clinical’ user who has project-specific access to the personal health information of project participants or patients.

Data Hosting and Security

EDGE data is hosted in Canada. EDGE-Alberta is hosted by Q9 Networks, which has data centres in Ontario (where EDGE is currently hosted), Alberta and British Columbia. Therefore, EDGE data may be physically located outside Alberta. Q9 Networks only provides the physical server used to host EDGE; it does not provide software, operating system or other logical support to the system. Access to the EDGE server is highly restricted by Q9.

Security measures for these facilities are routinely independantly audited. The audit report is confidential, but has been reviewed by EDGE and Alberta Innovates. The auditor found no exceptions.

Maintenance of EDGE software

EDGE technical administration (software maintenance) is the primary responsibility of the University of Southampton. EDGE organizational, operational and technological processes and procedures are required to comply with the requirements of ISO/IEC 27001:2005.

Disclosure Outside Alberta

EDGE is intended for use only by Alberta sub-licensees. There is no specific feature in EDGE to disclose health information outside of Alberta. However, since EDGE is accessed via an internet connection, it may be accessed from anywhere such a connection exists.

Information Security

EDGE organizational, operational and technological processes and procedures are required to comply with the requirements of ISO/IEC 27001:2005, as appropriate. Where relevant, UoS will use ISO/IEC 27002:2005 as a basis for auditing compliance with the relevant agreements and for investigating alleged breaches of privacy or security.

For more information or to request a copy of the Privacy Impact Assessment (PIA), please contact Trina Johnson at trina.johnson@albertainnovates.ca.