Validation Master Plan: EDGE Alberta

Prepared by: Ronda Danchak

Date: 16 August 2018

Version: 1.0

Document Approval

Name	Role	Date	Signature
Ronda Danchak	Author		
	IT		
	Validation		
	Client		

Version Control

Version	Author	Date	Description
1.0	Ronda Danchak	16 August 2018	EDGE Research Management System – Validation Master Plan

Table of Contents

1 Introduction

1.1 Objective

This Validation Master Plan (VMP) for EDGE Canada is to be used by sites who are managing Clinical Trial projects in EDGE. The Validation Master Plan defines the methodology, deliverables and responsibilities for supporting computer system validation and re-validation of EDGE.

1.2 Scope

This VMP applies to all staff responsible for sourcing, installing and implementing EDGE within Alberta for clinical trial purposes.

The Validation Plan for EDGE Alberta will include:

- The implementation of EDGE
- Where EDGE will be housed
- The software development life cycle (SDLC used)
- A definition of the post implementation validation and IQ

1.3 Definitions of terms:

Term or Abbreviation	Meaning
ACRC	Alberta Clinical Research Consortium
AI	Alberta Innovates
CSV	Computer System Validation
EU	European Union
GAMP	Good Automated Manufacturing Practice
GDPR	General Data Protection Regulation
IQ	Installation Qualification
IT	Information Technology
OQ	Operational Qualification
PQ	Performance Qualification
Q9	Q9 Networks, the company that hosts the Alberta instance of EDGE in Toronto. Q9 is owned by Bell Canada.
RA	Risk Assessment
Site administrator	The person designated by a sub-licensee to administer EDGE on the part of the sub-licensee. EDGE documentation sometimes also refers to this person as a super-user or local administrator.
SLA	Service Level Agreement

Sub-licensee	An organization licensing the use of EDGE from AI.
UoS	University of Southampton, the owner and technical administrator of EDGE.
URS	User Requirements Specifications
VMP	Validation Master Plan
VR	Validation Report

1.4 References

Version/Date	Title
19 June 2019	*Edge Clinical Research Management System – Privacy Breach Management Procedures*
2 August 2019	*Edge Clinical Research Management System – Services and Service Levels & Incident Response Procedures*
19 June 2019	*Edge Clinical Research Management System – Training and Awareness Procedures*
3 July 2019	*Edge Clinical Research Management System – Freedom of Information and Protection of Privacy (FOIP) Act Policy*
4 July 2019	*Edge Clinical Research Management System – Change Management Procedures/Development Requests*
19 June 2019	*Edge Clinical Research Management System – EDGE Security Specifications*
19 June 2019	*Edge Clinical Research Management System – Monitoring Procedures*

This document contains references to the following.

Version/Date	Title
Accessed 15 August 2018	FDA 21 eCFR Part 11
Accessed 16 July 2018	Health Canada Tri-Agency Statement of Principles on Digital Data Management
Accessed 16 July 2018	General Data Protection Regulation (GDPR)

2 Responsibilities

It is the responsibility of the Site Administrator to ensure the relevant individuals (IT, Quality Assurance, Operations Manager, etc.) are identified and notified of the CSV activities to be performed as per institutional policies

It is the responsibility of the Site Administrator, IT Lead, QA Lead and/or Operations Manager responsible for overseeing the validation to perform, check and sign the relevant sections of the validation documentation pertaining to their roles.

3 Assumptions, Exclusions and Limitations

3.1 Compliance Requirements

Validation of the system and related components will be based on compliance requirements referenced as 21CFR11 and any other applicable regulations. The core validation effort will consider requirements specifically as regulated by the US Code of Federal Regulations and the Health Canada Tri-Agency Statement of Principles on Digital Data Management.

Any organization that has customers in the European Union (EU), operates in the EU, or collects, uses or discloses personal information of EU data subjects should also ensure the system meets General Data Protection Regulation (GDPR) requirements.

3.2 Installation Qualification (IQ)

EDGE is cloud-based and therefore is not installed. EDGE uses Hyper Text Transfer Protocol Secure (HTTPS).

3.3 Operational Qualification (OQ)

The OQ confirms that the computer system can operate as expected, and that it meets the User Requirements Specifications (URS). The URS may not require full functionality of the system, and therefore the OQ should be a test for 'fit-for-purpose' based on these requirements. If at any time further functions are required, the system functionality must be qualified and documented before use.

3.4 Data Hosting and Security

Q9 is where EDGE UK hosts the Canadian instance of EDGE for Alberta Innovates and other groups. Q9 Networks 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. Bell and Q9 operate the country's largest network of data centres in Canada, providing the highest level of Colocation, Managed Services and Cloud solutions to organizations in support of their business-critical computing operations. Canadian privacy legislation defines personal information broadly as information about an "identifiable individual" or as information that allows an individual to be identified. Q9 does not collect, access or process any personal information that is stored by customers in their data centres. 100% Canadian data residency exists within Q9's high availability data centres. Mirrored secondary data centre sites are in a separate location with dedicated, high-capacity connections to their primary site. Security measures for these facilities are routinely independently audited. The audit report is confidential but has been reviewed by EDGE and Alberta Innovates. The auditor found no exceptions.

3.5 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.

Please contact EDGE Alberta with any questions or if you wish to receive a copy of the EDGE Alberta Policies and Procedures at edgealberta@albertainnovates.ca.

4 System Description

EDGE is a clinical research management software application that is owned by the University of Southampton (UoS) in the United Kingdom and licensed by Alberta Innovates (AI) on behalf of the Alberta Clinical Research Consortium (ACRC). AI sub-licenses the system to clinical sub-licensees in Alberta.

ACRC aims to enhance the quality and efficiency of clinical research and track the nature, extent and costs of clinical research. EDGE facilitates the standardization and streamlining of reporting on clinical research administration and related procedures. UoS in turn has contracted with Q9 Networks, a Canadian hosting company owned by Bell Canada, to host the EDGE system and the attendant. EDGE sits on a virtual machine in Q9 Networks in their Ontario location. Q9 states that it provides security services normally expected of an established data warehouse.

AI has only a limited role in the hosting and delivery of the system; those functions are retained by University of Southampton. Q9 Networks has a contractual relationship with UoS, not with AI. UoS is responsible to AI for ensuring the security and privacy of EDGE data hosted by Q9. It achieves this in part by retaining all control over the EDGE application; Q9 has no need to access EDGE data and is not involved in the administration of EDGE. It only provides the hardware used to host the data.

Q9 has in place strict procedures to monitor access, physical security, and environmental security in order to mitigate risk. All Q9 managed infrastructure is located within secured enclosures within the facility only accessible to key operational staff who require access in order to perform their job function. All access to the data centre, and enclosures within, is biometrically controlled. Access requires both a Q9 assigned access card and biometric authentication. All access is logged by the security system. Q9 provides multiple redundant power systems with a 100% Service Level Agreement (SLA) on continuous power.

The data centre is monitored 24/7 for both environmental and security issues. Servers are in a temperature-controlled environment. The environmental systems are all redundant and backed by diesel generators. The data centre is equipped with heat and smoke detectors. The primary system in place is a VESDA (Very Early Smoke Detection Apparatus) system.

Comprehensive back-up procedures exist in the case of need of disaster recovery, spare hardware will ensure that access will be uninterrupted. Q9 maintains back-up systems including electrical power, telecommunications and cooling and business continuity strategies and procedures intended to provide the continuing availability of the functionality of Q9's operations in the event of a disaster. Specifically, Q9's data centre operations are designed such that no individual Q9 data centre is dependent on another Q9 data centre for its continued operation in the event a disaster affects one of Q9's data centres. Q9 tests such systems, procedures and strategies on a periodic basis. Data will be encrypted on the server, such that any backup information cannot be read by Q9 without customer supplied encryption keys. Upon initial setup the customer will specify which files/directories should be backed up. The Q9 control center will perform regular backups, and only contact the customer in the event of an exception. Should a restore be required, the customer can contact the Q9 Control Centre and specify the data and target location for the restore.

The content of the EDGE system, at a high level, includes:

1. Information used to administer, manage and track clinical studies and research (e.g. quality improvement projects, contract progress, staff roles, patient accruals).

2. Financial information related to clinical research projects.

3. Information that allows the tracking and management of patient activities as follows:

    a. Personal employee information such as: user and clinical staff information (name, e-mail, address, training status, qualifications, and employee ID.)

    b. Personal health information, including demographic, diagnostic, treatment and care information. First and last names can be entered only as abbreviations of three characters each.

The EDGE application is designed to give a real-time view of clinical research activity, whether within a single institution or across research networks. It is a cloud-based clinical management system and allows information sharing between key stakeholders throughout the life of research projects. The EDGE application allows for the following functionalities:

1. Management of clinical health research studies.

2. Tracking of patient recruitment information.

3. Tracking, monitoring and auditing research governance.

4. Providing a shared, secured data repository for users to access.

5. Enabling reporting on Key Performance Indicators (KPI) (e.g., time-to-target, patient recruitment stats).

6. Providing a platform for improved resource management.

5 Validation Activity Requirements

5.1 Validation Approach

The validation methodology defines the quality management system for implementation of the system.

The design, development and unit/ initial system testing phases of the project and associated documentation will be carried out using the following methodology.

5.2 Validation Methodology

The following sub-sections describe the methodology utilized to validate the system.

5.2.1 Validation Master Plan (VMP)

A Validation Plan [this document] defines the scope of work (activities and deliverables) required to validate a system and identifies the design documents that will form the basis for: Installation and Operational and Production Qualifications. The VMP will describe the project, the system and the sequence of validation activities within the project.

5.2.2 Performance Qualification (PQ)

The PQ confirms that the installed computer system can be operated as expected by the end users for its intended purpose as detailed in the URS. (Ie. slowness of system, time system non-functional).

The PQ must be performed by the Site Administrator and other nominated end users who have been trained on the draft VMP (see OQ).

Each PQ step of the validation plan must be performed by an intended user and signed off as confirmation of completion. On completion of the PQ, the VMP can now be finalised by the Site Administrator taking into account any findings from the PQ.

Note: for Installation and Operational Qualification (IQ and OQ) see Assumptions Section (3.0) on page 6.

5.2.3 Validation Report

The purpose of the validation report (VR) is to summarise the results of the CSV as defined in the validation master plan. This should be written by the Site Administrator. It

should also detail procedures for change control, system review and decommissioning (see below).

If any sections of the validation master plan failed to meet the URS, this must be investigated to establish a resolution. If the problem cannot be resolved, the URS must be investigated to determine whether these are feasible, and whether all the requirements are necessary for the intended purpose. If the URS is adjusted the full CSV process should be repeated based on the new requirements.

The VR must then be reviewed and approved by the IT Lead, QA Lead, Operations Manager, PI and any other relevant authority.

The final approved validation report constitutes the authorization for release of the system for use. The master copy of the URS, VMP (IQ, OQ, PQ) and VR will be retained by the QA Lead, and copies will be issued to the Site Administrator for filing with the computer system documentation.

5.2.4 Validation Change Control

Any changes to the system hardware or software (including upgrades) will require all or some of the following documentation to be completed:

- Amendment to the URS
- Amendment to the Validation Master Plan
- Additional documented testing for these changes (may include repeat of original IQ, OQ and PQ)
- Amendment of the Validation Report

All of this documentation should be appended to the original CSV documentation and must follow the same review and approval procedure as above before any changes can take effect. The process for change control should be documented in the validation report.

5.2.5 System Review and Decommissioning

A periodic review process must be performed by the Site Administrator, QA Lead or both to verify that the computer system is still performing in accordance with the validation, operates in compliance with any applicable regulations and is being correctly utilised by the end-users and administrators.

This review should take place every two years from the initial validation or since the last revision/update of the system. This can be in the form of an audit. The process for

system review and decommissioning should be documented in the validation summary report.

Computer systems identified as no longer required or redundant, should follow a controlled, documented decommissioning process. Particular attention should be made to systems containing data, and where that data is not archived or may no longer be accessible if the system is decommissioned. In such a situation, migration and/or archiving of data should be considered, addressed and documented. Archiving may be in the form of printed paper copies of data appropriately labelled, signed and dated.

6 Acceptance Criteria

The system will be deemed acceptable when the Validation Report (VR) has been satisfactorily completed and approved and it states that the system is in a validated state. The approval of the VR includes the following criteria:

- It has been demonstrated that the User Requirements, as defined in the Functional Requirements Specifications, have been satisfied including that the system performs reproducibly and consistently within its full range of operating functionality.
- Risk should be mitigated for any identifiable potential problems. All known problems are documented and resolved if appropriate solutions can be found.
- Any constraints concerning the release of the system to production are documented.
- All essential documents have been adequately produced, reviewed, and approved.

7 On-going Validation Requirements

7.1 SOPs related to Validation and Development

The Validation Methodology will be conducted according to the list of institutional SOPs identified in the reference section. These SOPs will be used to cover the project activities and to provide a framework to ensure that the deliverables contain sufficient detail to allow validation of the system.

7.2 Data Preparation

Ensuring accuracy of data in the initial system is an essential part of validation. Initial population of system data will be sourced from the following classifications:

- New Static Data (data constants or look-up table values that are required by the new system but do not exist in current systems, verified for correctness before entry and after the data has been entered into the system).
- Existing Static Data (data constants that are manually or automatically converted from existing systems will be verified for correctness before entry and after the data has been entered into the system).

7.3 Ongoing Maintenance

The Validation Team will verify plans for maintenance of the hardware and software before the systems go live. The Validation Team will verify that each business department with responsibility for use of the system has change control in place before the systems go live.

7.4 Software Updates, Correction Packages and Patches

Upgrades or updates (including correction packages or “patches”) of the operating system software, database or Application software, with new versions, shall be assessed for validation impact through change control prior to use and consideration shall be given to re-validation of the system.

Approver	Name	Signature	Date
Principal User			
Operations Manager			
PI (if applicable)			
QA Lead			