EDGE Security and Data Protection Specification

This document outlines the security specification for the EDGE Programme and its contracted third parties. This document should be read in conjunction with both the EDGE Technical Specification and your EDGE contract / Service Level Agreement.

Author: Timothy Gibbons

Revision History		
Version Number	**Revision**	**Date**
0.1	First Draft	26/03/2021
0.2	Revised Third Party Supplier Table	29/03/2021
0.3	Updated Supplier Table	14/04/2021
0.4	Review	15/04/2021
0.5	Update Cloud Guidance & Images	16/04/2021
0.6	Independent Contractor Review	29/04/2021
1.0	Finalised – First version	19/07/2021
1.1	Update to include EDGE Canada	14/01/2022
1.2	Update of graphics & Telefonica	21/01/2022
2.0	Finalised – Second version	07/02/2022
3.0	Update references to EDGE 3	11/05/2023

Contents

Introduction

Purpose

The purpose of this document is to provide prospective and contracted subscribers of the EDGE Research Management software globally with information about all aspects of its hosting and security.

This specification includes information about the supplier and its contracted third parties, data protection adherence, compliance to country-specific requirements, such as those for the NHS in England, and national and international audits and data security standard certifications.

The CIRU

The Clinical Informatics Research Unit (CIRU) at the University of Southampton (UoS) provides a contracted subscription service for the EDGE Research Management software (The EDGE Programme).

The CIRU operates as an applied research and enterprise unit within the Faculty of Medicine at the UoS, employing academic and clinical staff across its five service groups. The Unit's core aims are:

• To undertake applied research in software development, data modelling and definitions, and develop terminology and standards.

• To provide software and services to those engaged in clinical research to improve quality and effectiveness, as well as drive new research questions within research data management.

• To support the delivery of improved healthcare through innovative informatics.

About EDGE

The core function of the EDGE Programme is to provide healthcare institutions delivering clinical research, either public or private, with web-based software tools and support all staff who manage research through a longitudinal research record. The underlying technology and cloud hosting of the software enables multiple departments and organisations to communicate and collaborate around a single national research record and research dataset.

Some of EDGE's core functions include:

- Participant Data Collection and Management, including SAE's, Finance, and Visits
- Private and shared document management
- Private and shared workflows for capturing internal processes
- Unlimited bespoke fields for Projects / Sites / Participants / Users
- Electronic delegation log
- Staff teams and training management
- Finance tracking (including organisational finance templates, budgets, and reports)
- Shared data collection, management, and reporting across multiple institutions
- Exceptional in-depth reporting capabilities

EDGE Cloud Hosting

The EDGE Programme is offered as an off-the-shelf product, fully contracted, managed, and hosted through the UoS. EDGE is a web-based Software as a Service (SaaS) solution and is not offered as an on-premise solution. The CIRU is responsible for ensuring the operation, security, and development of the software and access to the virtual environment.

There are multiple geographic instances of the EDGE Programme running across the globe, each with their own separate hosting environment specific to the geography that it serves. Subscriber data is never transferred between the geographic data centres, ensuring that subscriber data resides only in the physical location outlined in the subscriber's contract.

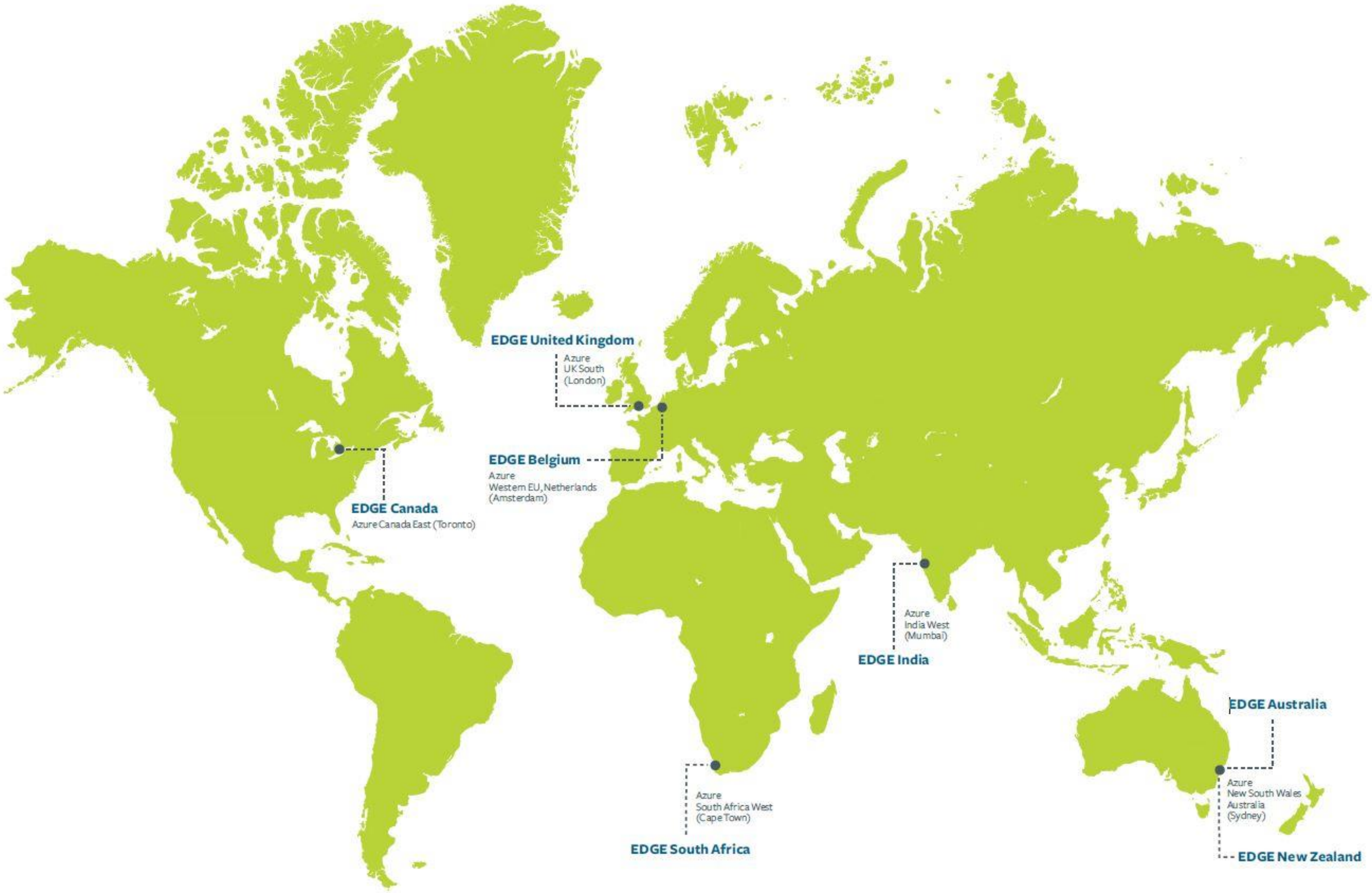
Microsoft Azure & Telefónica Tech

EDGE cloud hosting is provided through Telefónica Tech UK Ltd using the Microsoft Azure infrastructure. Microsoft Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centres.

Microsoft Azure is already providing infrastructure globally for healthcare organisations and the storage of participant identifiable information. Examples include the NHS Directory for NHS mail, which has been synchronised with the Microsoft Azure Active Directory (Azure AD), to allow the enablement of the Office 365 services for the NHS. Azure is also used outside of healthcare for the storage of sensitive information, such as for police forces across London and the Ministry of Defence.

Telefónica Tech UK is the CIRU's partner in delivering Microsoft Azure hosting as a managed service. As an experienced HSCN-approved Cloud Solutions Provider (CSP), Telefónica Tech has a proven track record in creating appropriate and secure infrastructure within Microsoft Azure for healthcare. Telefónica Tech has been selected as the CSP partner for the CIRU for their previous experience with working with UK NHS Healthcare Trusts and primary care in delivering new data hosting technologies and solutions. The CIRU has signed an GDPR-compliant Data Protection Agreement with Telefónica Tech UK for the provision of Microsoft Azure services.

EDGE MS Azure Hosting Locations



Supplier Data Processing Activities

	Role / Function	Signed DPA with UoS	Participant Data Processed	End User Data Processed	Purpose of Processing Operations under GDPR Article 4(2)
The University of Southampton, the CIRU	Supplier	N/A	☑	☑	Provision of EDGE Service Delivery EDGE Database Storage
TELEFÓNICA TECH UK	Cloud Solutions Provider (CSP)	☑	☑	☑	Provision of EDGE Service Delivery EDGE Database Storage
Microsoft Azure	Data Hosting Provider	☑	☑	☑	Provision of EDGE Service Delivery EDGE Database Storage
Salesforce	End User Helpdesk Software	☑	☒	☑	Provision of EDGE Service Delivery EDGE Helpdesk
Send Grid (Twilio)	Email Comms Provider	☑	☒	☑	Provision of EDGE Service Delivery EDGE Service Announcement Email

Supplier Certifications

Standard / Certification	NHS DSP Toolkit	Cyber Essentials/ Plus	ISO 9001 Quality Management	ISO 27001 Information Security	ISO 27017 Cloud Security	ISO 27018 Protection of PID in the Cloud	ISO 22301 Business Continuity	SOC II Type 2 Audit
The University of Southampton, the CIRU	☑	CE ☑	☒	☒	☒	☒	☒	N/A
TELEFÓNICA TECH UK	☑	CE+ ☑	☑	☑	☑	☑	☑	N/A
Microsoft Azure	☑	CE+ ☑	☑	☑	☑	☑	☑	☑
Salesforce Helpdesk	N/A	CE+ ☑	☑	☑	☑	☑	☑	☑
Send Grid (Twilio)	N/A	CE+ ☑	☑	☑	☑	☑	☑	☑

Appendix A

Sample Security Questionnaire

This appendix provides an overview of the most frequently asked security questions and our responses to each question. The questions have been grouped together under topics such as: third party suppliers, data storage and management, risk management, and vulnerability management.

Available on request

Appendix B

NHS Cloud Security Good Practice Guide Cloud Provider Responses (UK Only)

The NHS Cloud Security Good Practice Guide provides advice and guidance about the safeguards that should be put in place to enable health and social care organisations to safely locate health and social care data, including participant information, in the public cloud.

The CIRU has completed an NHS CSGPG template providing answers to all for both the CIRU and its hosting providers.

Available on request

Appendix C

Sample Data Protection Impact Assessment (UK & EU Only)

Article 35 of the UK General Data Protection Regulation (UK GDPR) requires that a Data Protection Impact Assessment (DPIA) is undertaken by the data controller where there are 'high risks to the rights and freedoms of natural persons resulting from the processing of their personal data'. A DPIA is designed to describe the processing, assess the necessity and proportionality of the processing, and to help manage the risks to data subjects. DPIAs are also important tools for demonstrating accountability, as they help controllers to comply with the requirements of the GDPR.

The use of Privacy Impact Assessments has become common practice in the NHS to achieve compliance with the NHS Digital Information Governance Toolkit (now the Data Security and Protection Toolkit) and DPIAs build on that practice.

The CIRU has provided a sample DPIA with responses to some of the most common questions on DPIAs as well as guidance on outlining how your organisation will use the EDGE Programme.

Available on request

Appendix D

Digital Technology Assessment (UK Only)

The Digital Technology Assessment Criteria (DTAC) for health brings together legislation and good practice in areas of clinical safety, data protection, data security, interoperability, and usability of applications. It is the new national baseline criteria for digital health technologies entering into the NHS and social care.

The DTAC is designed to be used by healthcare organisations to assess suppliers at the point of procurement or as part of a due diligence process, to make sure new digital technologies meet minimum baseline standards.

The CIRU has completed a copy of DTAC outlining the responses for the EDGE Programme.

Available on request

More Information

More information about data security and data protection can be found under the following resources:

EDGE Clinical Website

Telefonica Tech Website

Microsoft Azure Audits and Compliance

Microsoft Azure Security

Microsoft Azure International Regulatory

NHS Digital Cloud Guidance Overview

NHS Digital Cloud Security Frameworks

HRA Guidance for GDPR

ICO Guidance for GDPR

NHS Digital Guidance for GDPR

HRA Guidance for DPIAs