Data Protection Impact Assessment – INRstar and Engage self-care UK sub-processor transfer

LumiraDx Care Solutions

Document Number:	C-IS-REP-00043	Revision:	1.1
Information Classification		Public	

Contents

1. Purpose 3
2. Scope 3
3. Definitions 3
4. Referenced Documents 3
5. Data Protection Impact Assessment 3
5.1. Project Scope 3
5.2. Identify the need for a DPIA 3
6. Describe the Processing 4
6.1. Data Sourcing and Collection 4
6.2. Data Usage, Processing and Sharing 4
6.3. Data Deletion 4
6.4. Context of Processing 5
6.5. Vulnerable Groups 5
6.6. Ongoing concerns, public concern. 5
7. The Consultation Process 6
7.1. Stakeholder Commmunications 6
7.2. Project sign-off 6
8. Neccessity and Proportionality 6
8.1. Lawful basis of Process 6
8.2. Data Quality and Data Minimisation 7
8.3. Safeguards for International Transfer 7
9. Identify Risks, Identify Mitigations 7
10. DPIA sign-off and outcomes 7

1. Purpose

This document is a Data Protection Impact Assessment to support the migration of data from an existing infrastructure as a service sub-processor to a new public cloud infrastructure as a service sub-processor.

2. Scope

Data Protection Impact Assessment for the migration of INRstar UK, engage self-care UK services to a new UK based IaaS sub-processor.

3. Definitions

Please refer to document C-QMS-IND-00001 for definitions and abbreviations.

4. Referenced Documents

The following documents are referenced within this procedure:

Document Number	Document Title

5. Data Protection Impact Assessment

Explain broadly what the project aims to achieve and what type of processing of personally identifiable data it involves. It may be helpful to refer or link to other documents, such as a project proposal. Summarise here why the need for a DPIA has been identified.

5.1. Project Scope

5.1.1. This project is to transfer INRstar UK, engage self-care UK and associated services, including all data to a new infrastructure as a service (IaaS) sub-processor.

5.1.2. This project is being undertaken to:

a) Improve the confidentiality of information,

b) Improve the integrity and uptime of the applications,

c) Leverage improved application performance, application and security monitoring,

d) Align with improved infrastructure security measures,

e) Move to an IaaS subprocessor with a wider pool of technical expertise.

5.2. Identify the need for a DPIA

5.2.1. It has been identified a DPIA is required for this project as the data involved in this project shall contain identifiable data, special category data including data concerning healthcare as described under GDPR and the Data Protection Act 2018.

5.2.2. The data being processed is set out within the Privacy Policy and End User License Agreements for the respective products, available on the LumiraDx Care Solutions website or on request from an account manager.

5.2.3. The data may also have limited reference to individuals housed in prisons, mental health facilities or other sensitive care services.

5.2.4. Identifiable data may be linked within the INRstar application to gain limited reference to individuals providing healthcare to prisons, mental health services, high risk individuals.

5.2.5. LumiraDx Care Solutions UK Ltd consider this activity a large-scale processing of data, based on recital 91 guidance "large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational levels and which could affect a large number of data subjects and which are likely to result in a high risk".

6. Describe the Processing

Describe how the data will be collected, used, stored, and deleted. What is the source of the data? Will the data be shared with anyone? It may be useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will be collected and processed? How often? How long will it be kept? How many individuals are affected? What geographical area does it cover?

6.1. Data Sourcing and Collection

6.1.1. Data processed during this project shall be sourced directly from:

a) Existing data within INRstar UK and associated services,

b) Existing data within engage self-care app and associated services,

6.1.2. No additional data shall be collected, cross-referenced, or processed during this project.

6.2. Data Usage, Processing and Sharing

6.2.1. Data shall be processed to:

a) Generate anonymised data for test-runs of the transfer process to validate the clinical, quality management and information security management systems acceptance of the transfer.

b) To transfer the data to the new sub-processor (the project)

6.2.2. Data shall be accessible by a very limited number of individuals involved in the transfer project, the individuals haver undergone appropriate training, awareness of the project plan and are vetted as part of the recruitment and contract HR processes.

6.2.3. All data stored within INRstar, engage self-care and associated services shall be transferred.

6.3. Data Deletion

6.3.1. Access keys to decrypt original data sets shall be destroyed within 90 days of the project completion. This will render the data unreadable.

6.3.2. Data storage will be returned to a shared pool and overwritten over time.

6.3.3. A letter of attestation will be provided by the existing sub-processor to confirm the key deletion and over write.

6.3.4. Where copies of data are made during the project, the data, and where possible the data storage mechanism, shall be deleted after the transfer is complete.

6.3.5. All backup and disaster recovery data shall be deleted from the existing sub-processors systems no longer than 180 days from project completion.

Describe the context of the processing: what is the nature of the relationship with the individuals? How much control will they have? Would they expect their data to be used in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Have LumiraDx signed up to any approved code of conduct or certification scheme (once any have been approved)?

6.4. Context of Processing

6.4.1. LumiraDx Care Solutions UK Ltd is the manufactuer of INRstar CDSS and engage self-care products, in the context of this DPIA LumiraDx Care Solutions UK Ltd is a data processor operating on behalf of data controllers, primary healthcare providers and GP practices.

6.4.2. LumiraDx Care Solutions UK Ltd is the medical device manufacturer for INRstar.

6.4.3. LumiraDx Care Solutions UK Ltd is ISO 27001 certified.

6.4.4. LumiraDx Care Solutions UK Ltd is part of the LumiraDx Group.

6.4.5. The context of process (migration of data) is replacing one sub-processor (infrastructure as a service provider) for another sub-processor (infrastructure as a provider).

6.5. Vulnerable Groups

6.5.1. The vast majority of data held within INRstar and engage self-care is individuals receiving health care and is therefore considered to be part of a vulnerable group.

6.5.2. A small number of individuals may also be in other vulnerable categories, such as children, people with disabilities etc.

6.5.3. As the vast majority of individuals identifiable within the data are vulnerable, controls are in place to protect vulnerable data and be suitable for non-vulnerable or highly vulnerable individuals.

6.6. Ongoing concerns, public concern.

6.6.1. LumiraDx Care Solutions has not identified an on-going or public concern in the transfer of data between sub-processors for the improvement of application safety, security and integrity.

6.6.2. The NHS promote an architectural principle to operate health systems in the public cloud unless there is no clear reason to do so.[1]

[1] https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-architecture/principles/public-cloud-first#summary

7. The Consultation Process

Consider how to consult with relevant stakeholders: describe when and how other stakeholders will be consulted or justify why it is not appropriate to do so. Who else needs to be involved within your organisation? Are third party processors involved and is their assistance required? Is it necessary to consult information security experts, or any other experts?

7.1. Stakeholder Commmunications

7.1.1. A communications plan has been established to provide appropriate information to:

a) Data controllers, customer locations, and to provide information to customers to be passed on to patients on request,

b) Internal LumiraDx teams, senior management with responsibilities and the data protection officer,

c) Internal LumiraDx subject matter experts with appropriate technical and procedural expertise to ensure appropriate quality, clinical and security controls are adequate for this project.

7.2. Project sign-off

7.2.1. Project approval for the transfer of data shall go ahead once appropriate quality, clinical and security controls are assessed as adequate, sign-off shall be required from:

a) Chief Information Security Officer (LumiraDx Group)

b) Data Protection Officer (LumiraDx Group)

c) Head of Infrastructure (LumiraDx UK Ltd)

d) Medical Director (LumiraDx Care Solutions UK Ltd)

e) Clinical Safety Officer (LumiraDx Care Solutions UK Ltd)

8. Neccessity and Proportionality

Describe compliance and proportionality measures, in particular: what is the lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will function creep be prevented? How will data quality and data minimization be ensured? What information will be given to individuals? How will LumiraDx help to support their rights? What measures will be taken to ensure processors comply? What safeguards will be implemented for any international transfers?

8.1. Lawful basis of Process

8.1.1. Data controllers shall be notified of this project, and be provided a link to this DPIA prior to project initiation to allow appropriate time for data controllers and data subjects to request further information on the transfer of data.

8.1.2. Lawful basis determined per Article 6:

a) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.

b) processing is necessary to protect the vital interests of the data subject or of another natural person.

8.1.3. At all times, natural persons and data subjects can exercise their data subject rights through the data controller, or by contacting dpo@lumiradx.com.

a) In all instances, we will refer individuals to the Data Controller.

8.2. Data Quality and Data Minimisation

8.2.1. The INRstar UK, engage self-care UK and associated service data shall be copied and verified at each stage of the transfer process.

8.2.2. All copies shall be retained until the transfer is complete.

8.3. Safeguards for International Transfer

8.3.1. Data shall be not transferred outside of the UK.

9. Identify Risks, Identify Mitigations

The risk and impact assessment shall be conducted according to the LumiraDx Information Risk Management Methodology.

9.1.1. A risk assessment was conducted in-line with this DPIA.

10. DPIA sign-off and outcomes

Item	Name/Date	Notes
Measures Approved by	Alex Abbott 30/04/21	
Residual risks approved by	James Sharp, Head of Infrastructure Belinda Ehlers, Software Engineering Manager Alex Abbott, CISO, DPO	
DPO advice provided	Alex Abbott 30/04/21	
Summary of DPO advice: Migration can proceed on the basis that one of the key mitigating controls (integration of AWS logs into the SIEM and MSSP) is implemented immediately after the migration. Any delay in integrating AWS logs into the MSSP service will require a re-evaluation of the risk.		
DPO advice accepted or overruled by	Alex Abbott	
Comments: N/A		
Consultation responses reviewed by	N/A	
Comments: N/A		

The DPIA will be reviewed by		