Data Protection Impact Assessment (DPIA)

Project

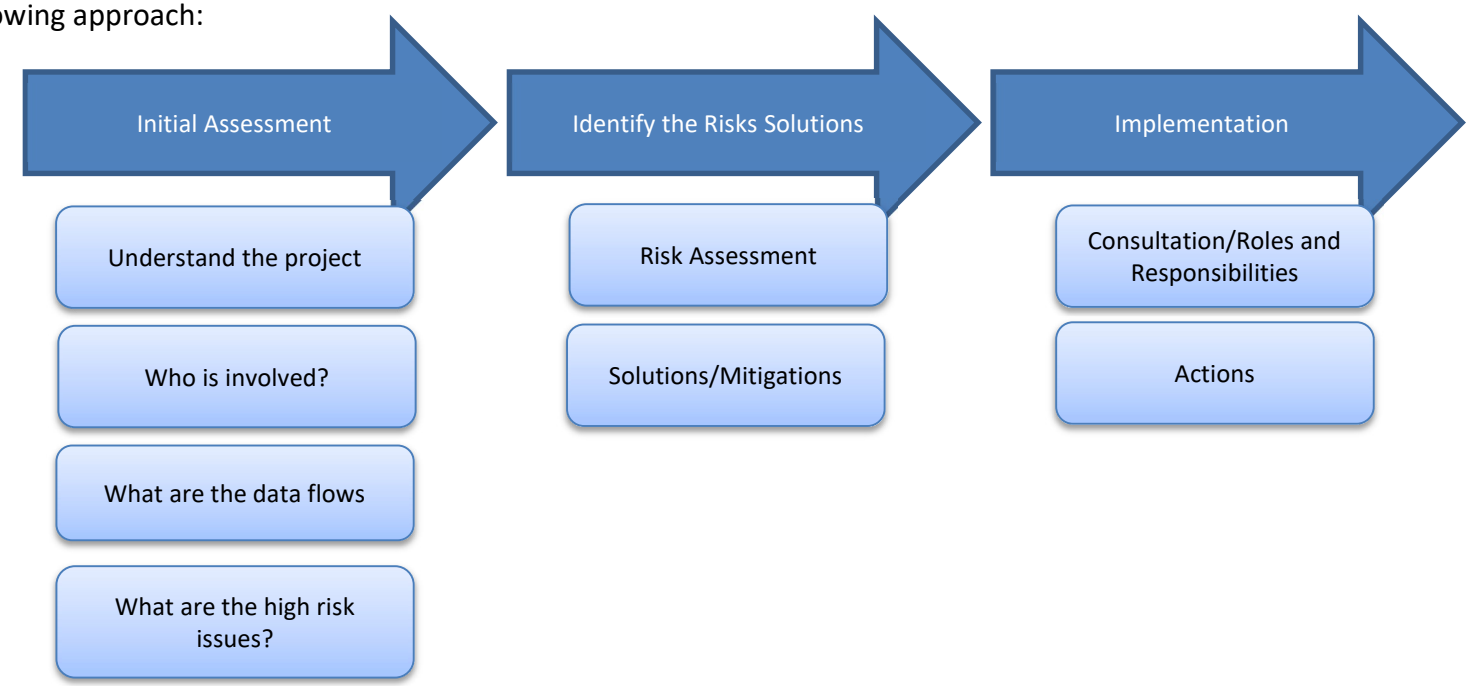
DPIA Name/Number: 159	Date: 07/06/2022
Owner: Douglas Bainbridge	Version: 1.2

1. Introduction

Because of the sensitive nature of the information that Here holds about individuals, it is highly likely that a DPIA will be required for most situations that involve processing of this information. This could include:

- Collection of new information about individuals
- Information about individuals being disclosed to organisations who have not previously had routine access to the information
- Use of information for a purpose it is not currently used for
- Use of new technology that might be considered intrusive
- Contacting individuals in a way that might be considered intrusive
- Data processed on a large scale
- Any form of automated decision making

Use of a DPIA is mandated under the General Data Protection Regulations (GDPR). This DPIA template is designed to be as simple as possible and uses the following approach:



2. Initial Assessment

Understanding the project

What is the project?
What are the benefits?
Has anyone done something similar before?

The First Contact Practitioner (Physiotherapist) program has embedded physiotherapists into GP practices. This data extraction project aims to provide reports and intelligence back to the practice/PCN detailing the impact of the physiotherapist.

This will involve extraction of some datasets from the GP IT system into the Here data warehouse for transposition and analysis.

The purpose of this work is to help the Practice leverage the data that it holds to support service improvement for patients.

Who is involved?

Internal or external parties?
What relationship (supplier, customer, partner)?
Who are the Data Processors and Data Controllers?
Practice are the Data Controller
Here are the Data Processor (on behalf of the Practice)

Here are processing data on behalf of the Practice, who have a legal basis for processing the information under Article 9 (2) h of the GDPR.

Necessity and Proportionality

What is the data? Personal Data/Sensitive Personal Data (See below). What are the flows of data? Where is the data stored? What retention periods apply?

In all cases only the pseudonymised patient identifier is used, without access to the Data Controllers Clinical System Here would be unable to re-identify patients.

The data extracted will be clinical codes (CTv3/CT2/SNOMED), limited to activity undertaken by a First Contact Physiotherapist

In all cases, the data remains the property of the Practice and will only be used in accordance with their instructions, and to support their work. There is no legal basis for Here to use or the data for any other purpose, or share it with any other party.

Primary data is held on the Practice clinical information system (TPP SystmOne /EMISWeb). Data will be provided to Here for processing by one of two methods:

I. Direct Submission by Practice via email
II. Automated Extraction using Strategic Reporting (SystmOne)

Any data extracts will be held securely on the Here data warehouse (Microsoft Azure cloud platform). All data will be removed upon contract end or on request by the Data Controller.

What are the Data Flows

Describe the flows and stores of information that are part of this project.

Data Flows should be mapped in the Data Flow Mapping Log \\nwxfs001\nwx-usf$\BICS Operations\Policies\BICS Policies\Governance\Information Governance Policy and appendices\Information Mapping\Data Flow Mapping.xlsx

High Risk Issues

What are the perceived high level risks resulting from this project? Such as -

- *Privacy intrusive purpose*
- *Automated decision making*
- *Technology*
- *Data categories (see below)*
- *Large scale processing*
- *Data transfers*
- *Individuals rights*

The following high-level risks have been identified:

1. Security of data transfers from the Practice to/from Here
2. Legal basis of data sharing not understood by all parties
3. Data Subjects are identified
4. Data retained longer than justified

3. Risk Assessment and Solutions

Risks Table

Identify the risks

No.	Issue	Description of Risk and why it arises	Potential Data Protection Impact	Level of Risk	Solutions
	Summary of relevant issue	*Description of risk*	*e.g. loss of personal data, breach of privacy, inappropriate sharing, individual rights*	*High, Medium, Low*	*Mitigation*
1	Security of data transfers from the Practice to/from Here	Risk of data loss in transfer/storage	Data security breach	Low	SR :- Data is held securely and is encrypted at rest. Full role based access controls apply. Data encrypted in transit through secure VPN between COIN and Azure platform. Data is held on UK based servers. Email Submission:- Data will be submitted to an email address on the @nhs.net email domain which is compliant with secure email standard (DCB1596) and is encrypted at both sender and recipient points.
2	Legal basis of data sharing not understood by all parties	Potential for complaint if data used inappropriately	Reputational damage or fine	Low	The legal basis for information sharing is stated in this document. Ensure all parties are aware.
3	Data Subjects are identified	Practices may inadvertently add Patient Identifiers into extraction	Data breach	Low	Reports for submission have been created to ensure only pseudonymised identifiers are used.
4	Data retained longer than justified	Data may retained longer than justified unless there is a clear process for disposal at end of pilot/project	Holding data unnecessarily presents a minor risk	Low	Data retained in accordance with Here Records Management Policy. Disposal of data should be included in any longer term contractual arrangement between Here and the Practice

Solutions Table

Accepted or adopted solutions. Cross reference to Risks Table (above)

No.	Agreed Solution	Residual Risk	Implementation Plan
Risk No.	*Summary of solution*	*Description of risk*	
1	Ensure data flows are included in Here data flow maps		
2	DPIA agreed by all parties		
4	Ensure data disposal is built into any longer term contract between Here/ the Practice		Include when longer term arrangements are known

4. Implementation

Consultation

The following parties have been consulted in the preparation of this DPIA:

Who?	Organisation	Position	Role/responsibility for this DPIA	Date
Matthew Riley	Here	Informatics Lead/Data Protection Officer		
Pete Strong	Here			

Action Log

Action	Description	Owner	Status

5. Definitions & Supporting Information

The following terminology should be used throughout this document to ensure consistent, legally recognisable definitions

Data Categories

'Personal Data' Data, which relate to a living individual who can be identified from those data, or from those data and other information, which is in the possession of, or is likely to come into the possession of, the Controller

'Special Category Data': Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life.

Controller v Processor

Controller: The Controller directs and has responsibility for the processing of information. In most situations Here will be the Controller.

Processor: The Processor processes information on behalf of the controller. The Controller has responsibility for the data and shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. (Art 28 GDPR).

A third, less common option is **Joint Controller**: Two parties take joint responsibility. This may apply if information is shared between two organisations to support reporting.

Lawfulness of Processing Information

As Controllers under GDPR, organisations that process personal data must establish and publish the lawful basis for the data processing.
The GDPR sets out conditions for lawful processing of personal data (Article 6) and further conditions for processing special categories of personal data (Article 9)

Under Art 6.1 of GDPR the most likely condition for healthcare provision are:

Article 6.1 (a) *the data subject has given consent to the processing of his or her personal data for one or more specific purposes*;*
Article 6.1 (b) *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

Article 6.1 (e) *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*

***Note:** (a) Consent is considered the weakest condition, and the most difficult to implement, and should be used as a last resort https://gdpr-info.eu/art-6-gdpr/

In addition, if Special Category Data is to be processed, one of the criteria under GDPR Art 9.2 must be satisfied. The most likely criteria for healthcare provision is:

Article 9 (2) h of the GDPR: processing is necessary for the purposes of preventative or occupational medicine, for the assessment of….medical diagnosis, the provision of health or social care or treatment of the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Art.9 para 3.

https://gdpr-info.eu/art-9-gdpr/

Note particular requirements around processing of information relating to children (Art 8 GDPR)

Legislation, Codes of Practices

The following legislation and codes of practice will apply to all DPIA's unless indicated otherwise

- General Data Protection Regulations (2018)
- Data Protection Act 1998 - http://www.legislation.gov.uk/ukpga/1998/29/contents
- Equality Act 2010 http://www.equalityhumanrights.com/publications/
- The NHS Constitution (DH, 2009)
  http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_113613
- Confidentiality: NHS Code of Practice (DH 2003)
  http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253
- The Caldicott Guardian Manual (DH, 2010)
  http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_114509
- The Information Governance Review (Caldicott 2)
  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

- Review of Data Security, Consent and Opt-Outs (National Data Guardian for Health and Care, 2016) Caldicott3 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF
- Records Management Code of Practice for Health and Social Care (Information Governance Alliance, 2016) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/547055/Records_Management_-_NHS_Code_of_Practice_Part_1.pdf
- Codes of practice published by the Information Commissioner http://www.ico.gov.uk/
- NHS Information Governance: Guidance on Legal and Professional Obligations (DH, 2007) http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_079616
- Guidance for Access to Health Records Requests (DoH 2010) http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/@ps/documents/digitalasset/dh_113206.pdf
- Access to Health Records Act 1990 http://www.legislation.gov.uk/ukpga/1990/23/contents

Policies and Procedures

The following Here policies and procedures will apply to all DPIA's unless indicated otherwise

IG Incidents	Here Incident Management Policy and Procedure
Complaints	Here Complaints Policy
IG Security	Here IG policy and appendices - Appendix 1 - Email Policy v5.0 - Appendix 2 - Internet Policy - Appendix 3 - Personal Computing Policy - Appendix 4 - Sussex-Wide Information Sharing Protocol - Appendix 5 - Transferring Personal Information Policy - Appendix 7 - Confidentiality Statement - Appendix 8 - Use of Equipment Off-Premises - Appendix 9 - Records Management Policy and Procedure - Appendix 10 - Information Risk & Data Breach Management Policy - Appendix 11 - Policy for Contacting Patients by SMS or Email - Appendix 12 - RA and Smartcard Policy v2.0 - Appendix 13 - Video and Photography Policy and Procedure - Appendix 14 - Staff Owned Portable Device Policy

	- Appendix 15 - Subject Access Requests Procedure - Appendix 16 - System Change Procedure - Appendix 17 - Pseudonymisation and Anonymisation Policy - Appendix 18 – Cyber Security Strategy
Training	Mandatory training policy - Data Security Awareness
Business Continuity	Here Business Continuity Plan

Version Control

Template Version	Date	Changes
0.1	28/11/2017	First draft
0.2	01/12/2017	Second draft
1.0	20/02/2018	Final version – signed off by IGOG
1.1	17/09/2018	Minor changes, clarification
1.2	24/12/2018	Minor changes/clarification
1.3	25/1/2019	Add Necessity and Proportionality section