Newcastle University

Information Governance for Health Research

Data Security and Protection Toolkit Framework

Document information	
Document name	Data Security and Protection Toolkit Framework
Author	Information Governance Team
Issue date	April 2022
Approved by	IGHR
Next review	October 2026

Document history		
Version	**Date**	**Summary of change**
0.1	05/10/2016	Introduction of Time frames
0.2	28/10/2016	Changes made to wording on diagram to reflect naming conventions and timeframe.
1.0	31/10/2016	Version approved by TG following amendments
2.0	24/07/2017	Update Flow diagram to reflect Enrolment
2.0	24/07/2017	Include Does my Project need an IGT decision tree
3.0	10/11/2018	Update Diagram and references to IGT to DSPT
3.0	10/11/2018	Update the flow to include reference to enrolment
3.0	30/11/2018	Formatting of diagrams.
4..0	15/03/2020	Update IGT to DSPT
5.0	29/03/2022	Update diagrams to include DPIA and different levels of approval involved. Change references to FMS IGHR
5.0	29/03/2022	Include a text description of the actual process
6.0	07/03/2025	Review of framework, no changes
7.0	17/10/2025	Complete refresh to reflect new procedure

Introduction

The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security, and that personal information is handled correctly. The University submits a toolkit annually to NHS England. Any university research project using Health and Social care data should use this document to determine whether they are required to be enrolled on the University Toolkit.

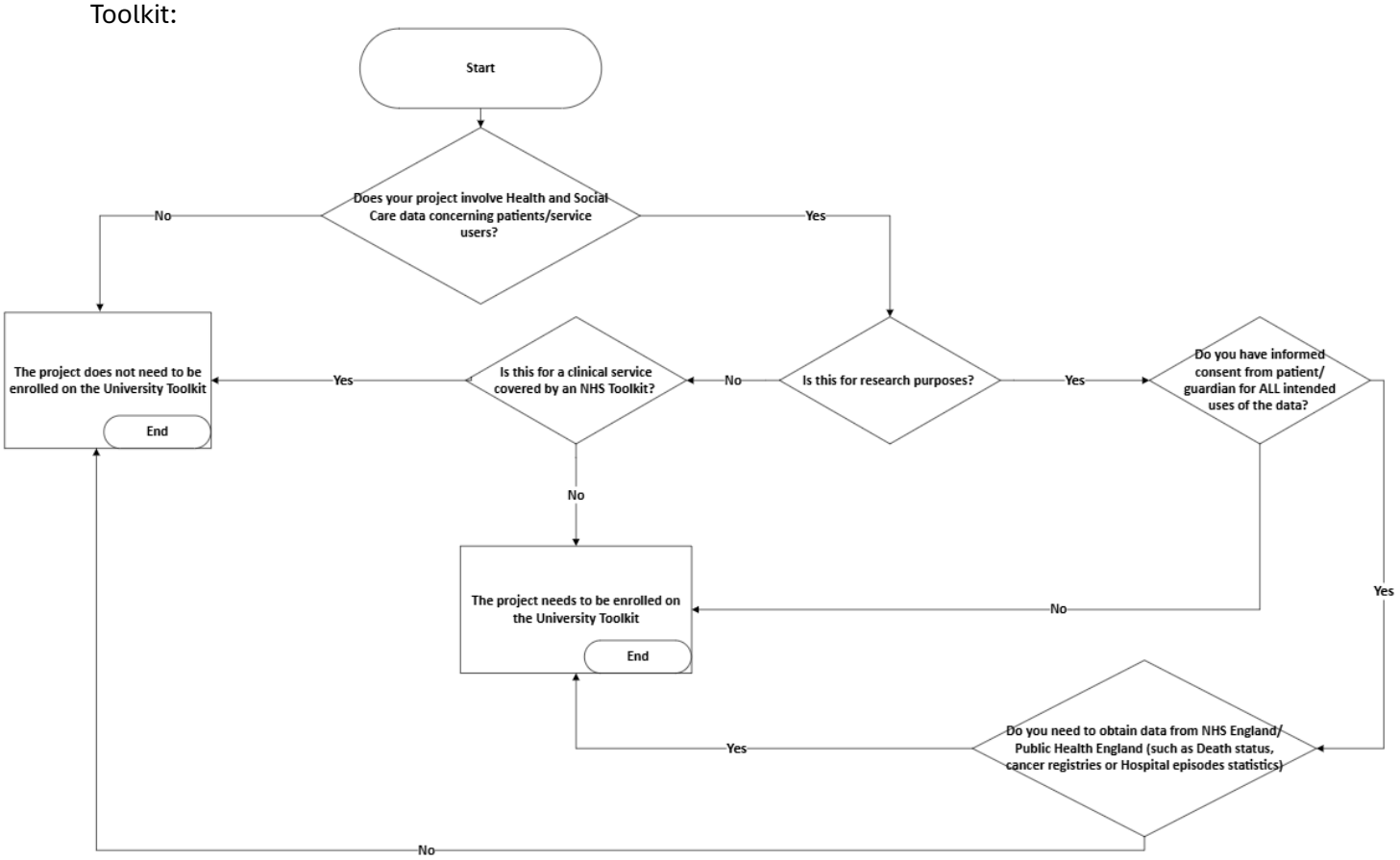
Does your project need to be enrolled on the Toolkit:

A project is required to be enrolled on the toolkit in the following instances.

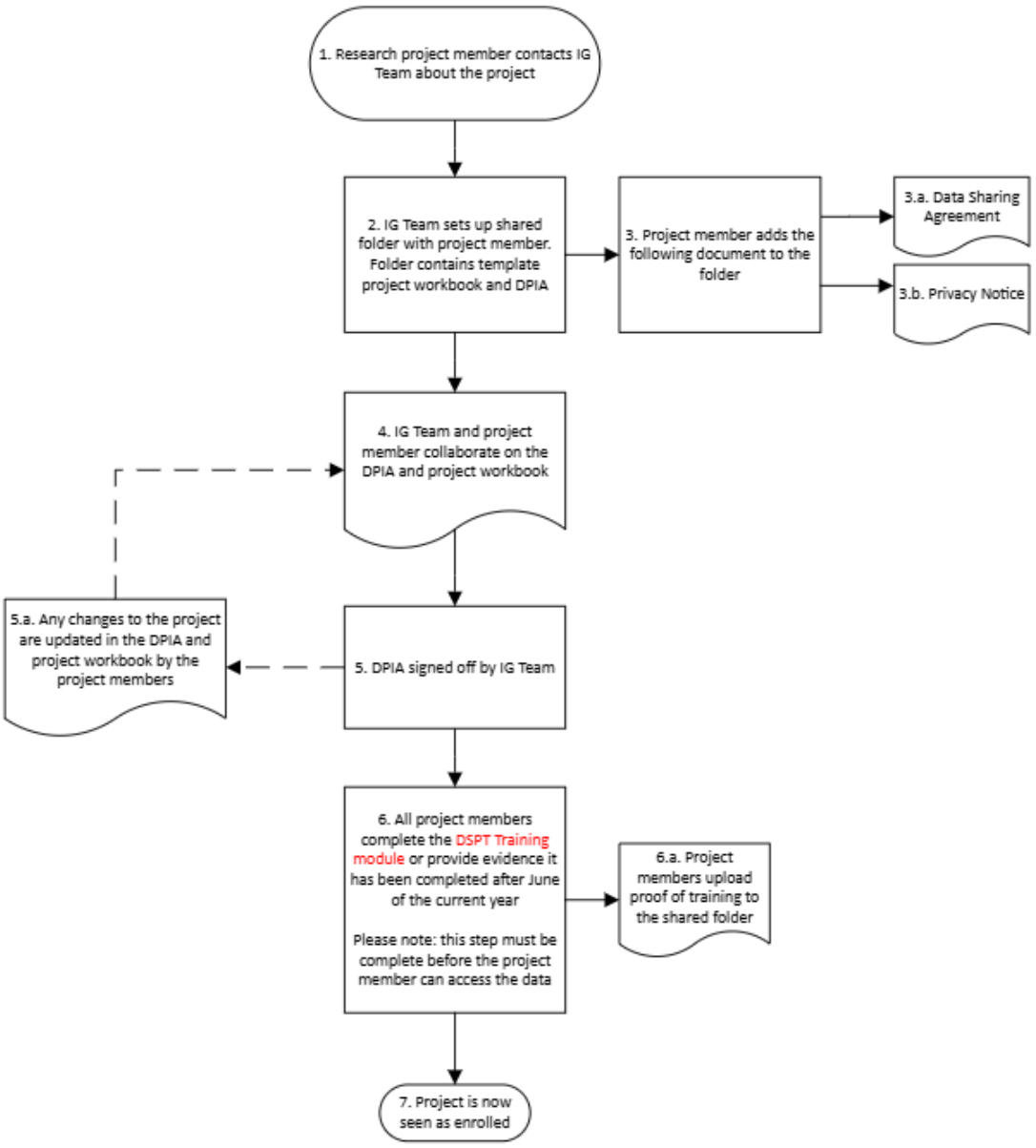
1. Access to confidential patient information without consent from the individual (Section 251)
2. Obtaining data from NHS Digital through Data Access Request Service (DARS)
3. Obtaining identifiable or pseudonymised patient data from another organisation (e.g. a University), that has data covered by S251
4. NHS and non-NHS organisations may also require a toolkit as part of a Data Sharing Contract or when you are carrying out work on behalf of an NHS organisation eg Clinical Trials or performing testing or audits.

The following link contains contact details for advice from NHS England on the Toolkit: https://www.dsptoolkit.nhs.uk

The decision tree below can be used to help determine if the project should be enrolled on the Toolkit:



Project Enrolment Process



1. Where a project member has identified a project that needs to be enrolled onto the University Toolkit, they should contact the Information Governance Team via rec-man@newcastle.ac.uk

2. The shared folder will be set up on the Information Governance SharePoint site and access will be given to relevant project members as required.

3. a. All versions of data sharing agreements for the project should be held in this folder. This includes the data sharing agreement from the organisation providing the data (e.g. NHS England), as well as any other organisations collaborating on the project (e.g. other universities)

b. All versions of privacy notices for the project should be held in this folder.

4. Project Workbook
   This contains the following pages:
   - Project Enrolment - This records details of the Principal Investigator, and reference numbers for related documentation such as NU Projects, DARs, CAG and any other applicable.
   - Project Member List - Used to document which staff members are working on the project, their contact details, location, working arrangements and their access to the data.
   - Information Asset Register – this should detail any information assets held that are relevant to the project. An information asset is a body of information which has value to the project. For example, records stored in a filing cabinet, cloud-based storage, software, PC's, Laptops, file shares, external hard drives, USB flash drives etc.

5. DPIA (Data Protection Impact Assessment)
   This is a risk assessment used to identify and mitigate or manage any data protection risks identified within the project. This will be signed off by the IG Team, however it is a live document and should be continuously updated during the lifecycle of the project to reflect any changes.

6. DSPT Training

This should be completed annually by all project members (internal and external) who have access to the project data. It can be accessed by internal project members via the University Learning Management System (LMS). For external project members who are unable to access the LMS, the IG Team will send them a copy of the Toolkit Handbook, and the project member should confirm in writing to rec-man@newcastle.ac.uk that they have read this.

The University also requires that all staff complete Information Security Mandatory Training every 2 years.