Data Protection by Design & Default Procedure

Completion of Data Protection Impact Assessments

November 2020

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email HULLCCG.contactus@nhs.net, or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.

Name of Policy:	Data Protection by Design & Default Procedure
Date Issued:	November 2020
Date to be reviewed:	November 2023

This policy will impact on:	All Staff	
Policy Area:	Information Governance	
Version No:	3.0	
Author:	Information Governance Team	
APPROVAL RECORD		**Date:**
	Information Governance Steering Group	11/11/20

Data Protection by Design & Default Procedure

Contents

1 Introduction

The latest Data Protection legislation requires organisations to maintain a privacy by design approach to the processing of personal information. This is to be achieved by the implementation of a range of appropriate technical and organisational measures to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible and that processing is transparent in accordance with the Data Protection legislation principles.

The Information Commissioner's Office has increased powers of audit within organisations and can fine organisations up to the equivalent of 10 million euro's for administrative infringements such as not having appropriate procedures in place to manage the use of personal identifiable information.

This procedure describes the CCG's approach to privacy by design, to ensure that all staff are aware of the approach that should be taken when processing personal information.

2 Data Protection Impact Assessment

Data Protection Impact Assessments (DPIAs) are required under Data Protection legislation where the use of personal information is likely to result in a high risk to the rights and freedoms of individuals, particularly where there is large scale processing of sensitive information, such as health information, or where the processing is automated.

The CCG has a Data Protection Impact Assessment Procedure in place which must be followed to demonstrate that privacy concerns have been considered and to assure the CCG regarding the security and confidentiality of personal information.

The DPIA Procedure contains questions which cover all the Data Protection principles and prompt Project Managers/Leads to consider:

- whether all personal information is adequate relevant and necessary
- how the personal information will be kept up to date and checked for accuracy
- whether personal identifiable information is required, or whether this could be pseudonymised
- the legal basis for processing the personal information
- transparency requirements, such as how individuals will be informed of the use of their information including rights such as rectification, restriction, objection, access,
- whether there is an audit function, to report who has accessed the information
- how the personal information will be transferred
- how/where the personal information will be stored
- the security of the transfer, storage and access to the information
- retention and destruction arrangements
- business continuity arrangement
- whether the personal information will be transferred outside the EEA

The DPIA procedure includes the requirement for review by the CCG's Data Protection Officer and prior notification with the ICO, where applicable.

3 Pseudonymisation

Under Data Protection legislation there must be a legal basis to process personal information, with additional conditions required when processing sensitive information, such as health information or ethnicity.

Even where there is an identified legal basis, the principles of Data Protection legislation mean that the use of personal information should be minimised and protected, and pseudonymisation, where possible, facilitates both data minimisation and security.

Pseudonymisation involves the removing of identifiers from patient data so that patient/service user may not be identified. The aim of pseudonymisation (vs anonymisation) is to be able to collect additional data relating to the same individual without having to know the identity so that it is possible, for example, to analyse data sets and trends over time. Individual service user activity should be able to be identified but not the service user themselves. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index.

Pseudonymisation can be likened to anonymised information in that, in the possession of the holder, it cannot reasonably be used by the holder to identify an individual. However, it differs in that the original provider of the information may retain a mean of identifying individuals.

Under Data Protection legislation, information that has been pseudonymised can still be considered as identifiable (and therefore within the remit of the legislation) if identification is possible to those who do not have access to the pseudonymisation key by using additional information. To determine whether an individual is potentially identifiable following pseudonymisation, account should be taken of all means reasonably likely to be taken if re-identification was attempted.

Current pseudonymisation controls on data flowing to Hull CCG are NHS Digital approved tools and are applied at source by the Data Services for Commissioners Regional Office (DSCRO) the provider of our Risk Stratification tool.

Before personal information is processed within the CCG, staff must consider whether the purpose can be achieved with pseudonymised information.

4 Record of Processing, Information Asset Register and Dataflows

The CCG has updated the Information Asset Register and Dataflow Maps in line with the requirements of the new Data Protection legislation. These now include mandatory safeguards, additional security measures in place, whether access logs or auditing is available and the retention period.

All existing Information Assets and Dataflows prior to the new Data Protection legislation have been documented on the updated Asset and Dataflow Maps in line with the new requirements.

A Procedure for the Review of Asset Register and Dataflow Risk Assessments has been developed and is now in place for Information Asset Owners to undertake reviews of their Information Assets and Data flows on a quarterly basis to ensure risk assessments are reviewed on an ongoing basis and to maintain the confidentiality, integrity, availability and resilience of the Information Assets at the CCG.

Any new Information Assets or processing activities identified during the review process are added to the Information Asset and Dataflow Maps and risk assessed accordingly.

5 New Processing Activities

A Data Protection Impact Screening Assessment must be completed when new projects, processes and contracts are to be implemented, or where existing processes are to undergo changes that will affect how personal identifiable information is collected and processed, in order to identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy.

This includes:

- Where the CCG will receive and process Personal Confidential Data (PCD)
- Where the CCG is signatory to a contract that facilitates to the processing of PCD e.g. a contract to facilitate a service or function by GP Practices.
- Further assurance is required due to third party involvement or other complicated situations.
- Movement of services who process PCD to new premises

An Information Asset Owners Handbook is in place which details the responsibilities of project managers in completing a Data Protection Impact Assessment and when responsibilities are to be passed to the relevant Information Asset Owners, in order that an up to date Information Asset Register can be maintained.

6 Process

At the start of a project or commissioning of a new service, or implementation of a system the Project Manager / Lead must complete the screening questions of the Data Protection Impact Assessment (DPIA), to ascertain whether the project will involve the new processing or any change in processing of PCD and whether a full Data Protection Impact Assessment is required. This must also be completed when significant changes occur to an existing project, service or system where it will affect or change the way in which personal confidential information is collected and processed. A section has been added to the Report Template to remind staff that a DPIA must be considered.

If the answer to all the screening questions is NO, i.e. no PCD will be processed in order to develop and implement the project, service or system then this should be confirmed at the bottom of the Screening Questions. If required an Information Asset Owner should be

identified and a new Information Asset Risk Assessment and/or dataflow should be completed so that the Information Asset Register can be updated.

The screening questions must then be submitted to the Information Governance Group to confirm the outcome is appropriate.

If the Answer is YES to any of the screening questions or the review by the Information Governance Group requires it then a full DPIA must be completed and submitted to the Information Governance Specialist to allow a full risk assessment of the use of personal confidential information within the project.

Completion of the full DPIA should identify the Information Asset Owner, who is then responsible for adding the projects information assets on the CCG's information Asset Register and completing the Data Flow Map and checking whether there is an impact on the CCG's Privacy Notice.

A report indicating potential risks and areas to be addressed will be prepared and returned to the project manager for agreed action and the CCG IG Lead copied in. The Project Lead must complete the agreed action within the risk assessment and return it to the Information Governance Specialist for assessment of appropriateness of actions agreed. This should be saved in the project folder by the Project Manager/Lead. All subsequent updates or DPIA-related documentation should be saved here and dated appropriately after being submitted to Information Governance Specialist for re-assessment.

Once appropriate action has been determined and recorded in the risk assessment report by the project lead, the original DPIA and the risk assessment report will be submitted to the CCG's Data Protection Officer (DPO) for review.

If the DPO is satisfied all risks have been identified and appropriate mitigating action agreed to be implemented then they will sign off the risk assessment and it will then go to the CCG SIRO or Caldicott Guardian for sign off.

If the DPO is not satisfied all risks have been appropriately addressed then this will be raised with the CCG SIRO to prompt appropriate mitigating controls to be established and implemented. It should be noted that if significant risks are not appropriately mitigated then the DPO is duty bound to consult with the Information Commissioners Office.

The Project Manager/Lead, or identified Information Asset Owner, is responsible for keeping the DPIA under review until the project is completed. As projects can change throughout their implementation, it is important that all changes that affect the processing of personal information must be reported via the DPIA as they are identified to enable re-assessment of all processing of personal identifiable data. Any changes made to a DPIA must be reported to the Information Governance Group to provide the CCG with on-going assurance that the appropriate parts of the DPIAs have been completed for all projects and supports on-going monitoring.

The Information Governance Specialist will maintain a register of all new projects underway and due to commence, detailing the completion position of the DPIA to put to each Information Governance Steering Group. This is provide the CCG with on-going assurance that the appropriate parts of the DPIAs have been completed for all projects and supports on-going monitoring.

7 Relevant Documents

- Data Protection Impact Assessment Procedure
- Information Asset Owners Handbook
- Record of Processing/ Information Asset Register