DATA PROTECTION IMPACT ASSESSMENT (DPIA) POLICY

Introduction

This policy reinforces the principles of Information Governance and Data Protection. The document outlines the Practice's approach and methodology for Data Protection Impact Assessments for new and existing systems and processes.

It is important that all new processes, policies, projects, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements.

The policy details the process to be followed to ensure a formal assessment is completed to determine whether any proposed changes to the Practice's processes, policies, projects and/or information assets impacts on the integrity and accessibility of personal information.

Some of the considerations that should be taken into account are whether a new process, project or information asset will:

- Affect the quality of personal information already collected;
- Allow personal information to be checked for relevancy, accuracy and validity;
- Incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required or in accordance with The Records Management: NHS Code of Practice;
- Have an adequate level of technical and organisational security measures to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage;
- Enable data retrieval to support business continuity in the event of an emergency;
- Enable the timely location and retrieval of personal information to meet a subject access request; and
- Alter the way in which the Practice captures information within / monitors information from a key system.

The rationale for conducting a DPIA is to:

- Identify and manage risk;
- Avoid unnecessary costs and inadequate solutions;
- Avoid loss of trust and reputation;
- Inform the Practice's communications strategy; and

- Meet legal requirements in terms of information security, data protection and confidentiality.

The policy applies to information held in both manual and electronic form.

This policy applies to all staff who work for the Practice including contractors, who are responsible for project managing a new project, implementation of a new process or plan to modify a current system (information asset).

Data Protection Impact Assessment (DPIA) Process

A DPIA must be carried out in addition to compliance checking or a data protection audit, and conducted at a stage when the outcome can genuinely affect the development of a project or process.

An effective DPIA will help identify and avoid problems which may not be obvious at the conception stage and should form an intrinsic part of the overall risk assessment.

When should a DPIA be undertaken?

Not every new project, system or change in process will require a DPIA. The Information Commissioner's Office (ICO) recommends that DPIAs are completed to comply with a change in law, introduction of new or intrusive technology or where person identifiable or sensitive information which was originally collected for a limited purpose is going to be collected for any new purpose(s) or reused in a new and unexpected way.

Completion of the initial DPIA Screening Questionnaire (Appendix 1) will ensure that a full DPIA is completed only when necessary and provide evidence to support the Practice's Information Governance agenda.

Best practice dictates that the initial screening questionnaire should be started when:

- The project / process is being designed and the scope has been agreed;
- Before a system has been procured;
- Before contracts/MOUs/agreements have been signed.
- For all QIPP projects as a mandatory assessment within each Project Initiation Document (PID)

Who Is Required to Complete a DPIA?

The initial screening questionnaire should be completed by the Information Asset Owner (IAO) or delegated to the individual responsible for overseeing the implementation of the project / process / policy / amendment to an existing system (such as the project manager); the Senior Responsible Officer (SRO).

Applying the Outcome of the Initial Screening Questionnaire

Where answers to questions are 'Yes', a full scale DPIA should be completed with support from the Data Protection Officer.

Definitions

Data Protection Impact Assessment	A risk technique mandated by the General Data Protection Regulations to enable organisations to address privacy concerns and ensure appropriate technical and organisational safeguards are addressed and built in to new projects / processes / policies / amendments of existing systems
Projects / processes / policies / amendments of existing systems	DPIAs are required when new projects occur (e.g. introduction of a new electronic patient record, process involving the transfer and/or use of information between providers of a service) or where plans are proposed to develop an existing information asset. These can be both paper and electronic.
Special Category data	Under the Data Protection Act this is data such as patient diagnosis, medical history, ethnicity, sex, religion.
Personal data	Data which is capable of identifying an individual, but isn't classified as special category data, for example, name, postcode, GP, next of kin, address, date of birth and so on.
Privacy-invasive technology	Privacy-invasive software is a category of computer software that ignores users' privacy and that is distributed with a specific intent, often of a commercial nature/mass marketing, which negatively affects its users. Examples include, but are not limited to, locator technologies such as global positioning systems (GPS) and mobile phone locators, biometric scanners.

Roles and Responsibilities

The Governing Body

The Governing Body owns the information governance strategy & framework and the implementation of measures to minimise information risk and safeguard the interests of its staff, patients and information assets of the Practice.

Senior Information Risk Owner (SIRO)

The SIRO is responsible to the Governing Body for ensuring an Information Governance strategy & framework is implemented, reviewed and its effect monitored. Privacy Impact Assessment is one element of the management of IG and information risk.

The SIRO will:

- Take ownership of the Practice's information risks;
- Act as the advocate for information risk on the Governing Body;
- Provide written advice to the Chief Officer, as detailed in the Annual Governance Statement; and
- Occupy a key role in ensuring effective management and identification of information risks.
- Oversees all QIPP projects and ensure they have a completed PIA

Information Asset Owners

An Information Asset Owner has responsibility for managing aspects of the Practice's business, and therefore will be responsible for knowing what information assets are held by their team, understanding the potential risks to the assets and to provide assurance to the Practice's SIRO concerning the security, confidentiality, integrity and use of the assets. Their roles include:

- Understanding what information is held;
- Knowing what is to be added and removed;
- Knowing how information is moved / transferred;
- Knowing who has access and why; and
- Ensuring compliance with the relevant legal frameworks, i.e. consent and confidentiality

Information Asset Administrators

As an Information Asset Administrator, with day-to-day responsibility for the creation, receipt, use and storage of information assets, IAAs will provide support to the Information Asset Owner for their team to ensure that:

- The Information Asset Register is kept up to date
- Policies and procedures regarding information management and risk are followed
- Actual or potential information risks are recognised and reported; and
- Information sharing agreements are complied with.

Data Protection Office (DPO)

The DPO is responsible for assessing and manage the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing. This will be achieved by reviewing the outcome of the DPIA to ensure compliance with the GDPR and national data protection legislation is maintained.

Monitoring and Review

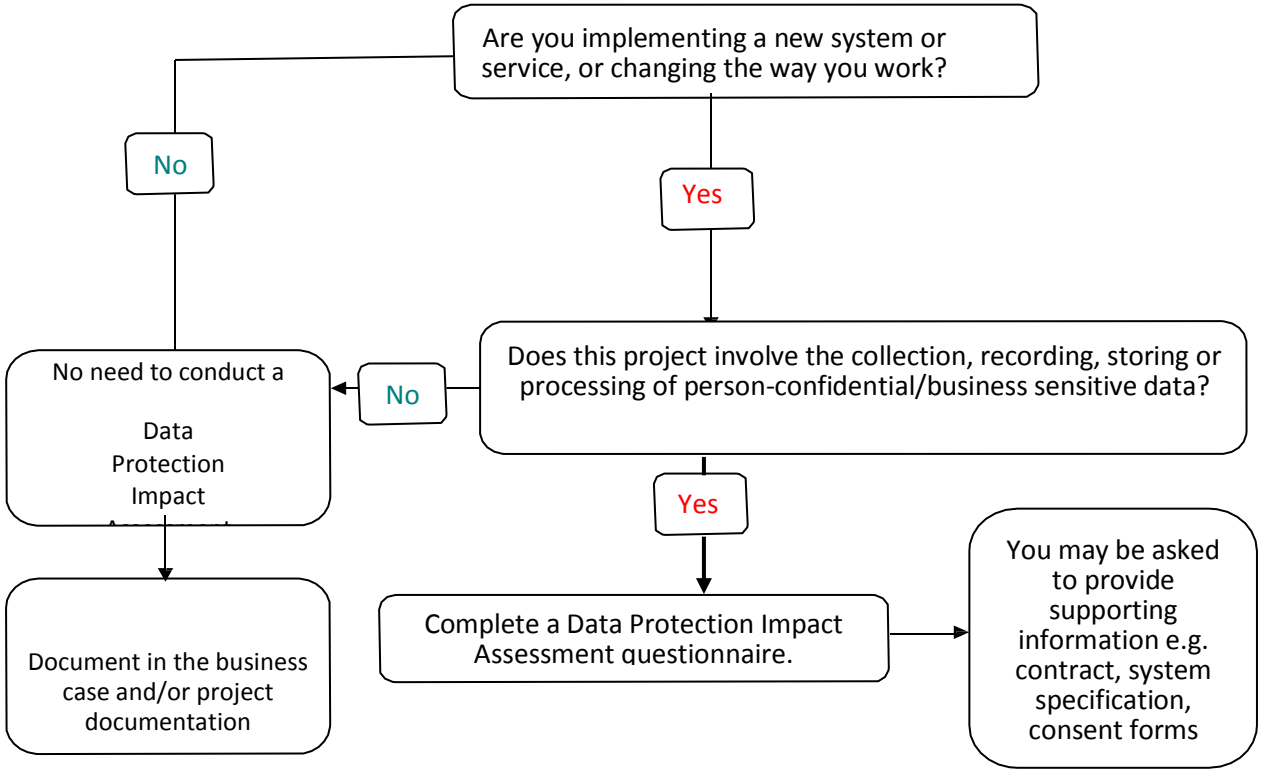
The Chief Finance officer, as SIRO, will receive regular reviews of information risk to support their written advice to the Chief Officer and will review all PIAs as part of Project Initiation Documentation (PIDs)

The Audit Committee will formally monitor the implementation and performance of this policy by:

- reviewing progress against the IG Toolkit/DSP Toolkit;
- considering IG risk mitigation plans;
- ensuring a programme of internal/external audit reviews (including audit of the IG Toolkit/DSP Toolkit self-assessment); and
- monitoring the implementation of audit recommendations.

This policy will be reviewed annually by the Practice's IG Working Group, or sooner should changes in legislation or guidance require it.

Appendix 1 - Do I Need to Complete a Data Protection Impact Assessment questionnaire?



When deciding whether a DPIA questionnaire is required, if the first answer is 'yes', but the second response is 'unsure', please complete the questions in section 1 of the DPIA questionnaire to assist the decision. Further guidance can be sought from the Data Protection Officer.

The questionnaire will be reviewed by the Data Protection Officer, and the recommendation from the questionnaire will be notified to the Project Manager / Information Asset Owner. The recommendation will be either:

1. A full DPIA is required where the new process or change of use of PCD/Business Sensitive data requires more thorough investigation; or
2. The DPIA questionnaire will be signed off by the Data Protection Officer, the PIA log updated by the Data Protection Officer and the outcome reported to the IG Working Group.