Version	Date Reviewed	Next Review Date	WIMBLEDON MEDICAL PRACTICE
2.1	January 2020	January 2021	

DATA PROTECTION IMPACT ASSESSMENT (DPIA) POLICY

Consideration should be taken into account where a a new process, project or information is applied to ensure the following does not;

- 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.

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).

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.

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.

Monitoring and Review

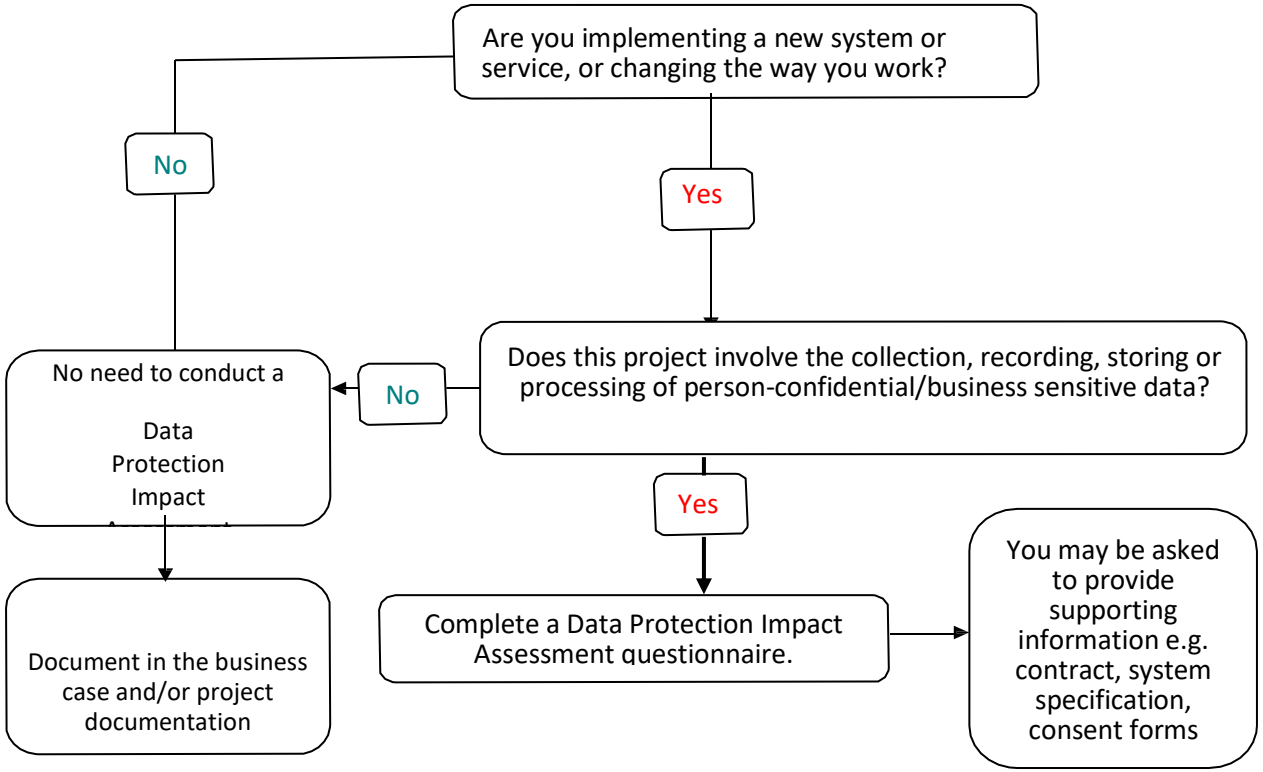
The Chief Finance officer, as SIRO, will receive regular reviews of information risk to support their written advice to the Chief Officer and will review all PIAs as part of Project Initiation Documentation (PIDs)

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.