INFORMATION GOVERNANCE 33
DATA PROTECTION IMPACT ASSESSMENTS

1. This briefing looks at the development of Data Protection Impact Assessments (DPIAs) and addresses how and when they should be completed. A comprehensive background to them can be found on the Information Commissioner's Office (ICO) website[i].

2. The DPIA should not be seen just as a document to be completed but rather as a process to be followed. The objective is to identity and review any risks relating to the processing of personal data and ensure that the Data Controller is managing them appropriately. DPIAs have been around for some time, occasionally called Privacy Impact Assessments, but since the introduction of UK GDPR they are now a legal requirement for certain types of data processing.

3. The definition of the type of processing that will legally require a DPIA is where it is "likely to result in a high risk to the rights and freedoms of data subjects". This means any major new processing, such as that required for the COVID pandemic which was done at national level, or the development locally of a new clinical service will require one. A DPIA is also required for a significant change to an existing processing, such as a practice changing from one clinical system supplier to another, or the installation of a new telephone or CCTV system.

4. The process to follow for the completion of a DPIA has several defined steps[ii]:
    - Identify the need
    - Describe the processing
    - Consider consultation
    - Assess necessity and proportionality
    - Identify and assess risks
    - Identify measures to mitigate risk
    - Sign off and record outcomes

5. To assist in the DPIA process there are a number of templates available, such as this one from the ICO[iii], and this one that N3i have produced[iv]. Other organisations such as NHS Digital and local CCGs may also have templates they use. There is no legally approved template, the choice is down to the Data Controller, ie the GP Practice. Their purpose is to guide you through the process by prompting you with the right questions to be asking and to create a record of the process itself and the decisions taken. The completion of a DPIA will generally involve input from several parties such as system suppliers, national bodies like NHS Digital, and local IMT providers, as well as data protection specialists.

6. Finally, it is for the Data Controller (the GP Practice) to formally approve the DPIA following advice from their Data Protection Officer.

---

[i] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
[ii] https://www.itgovernance.co.uk/blog/gdpr-six-key-stages-of-the-data-protection-impact-assessment-dpia
[iii] https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx
[iv] https://ig.n3i.co.uk/newsletters/n3i-dpia-template.docx