Resource Pack 17 - Privacy Impact Assessment

Any new project that involves the potential use of person/ patient identifiable data must involve the Information Governance Lead at the outset. Where the project involves patient information, the Caldicott Guardian must also be involved. Part of the formal process must be the privacy impact assessment that identifies any areas of concern in relation to the identifiable information. The Information Commissioner has developed a Privacy Impact Assessment (PIA) handbook that will assist organisations to ensure that privacy concerns and safeguards are addressed and built in as a project or system develops. The handbook can be found externally via the Information Commissioner's website and gives full and explicit details about why and how to conduct a full or small scale privacy impact assessment, and Data Protection compliance.

Privacy impact assessments are not mandatory but are increasingly being required under government policy (outcome from O' Donnell report following Her Majesty's Revenue and Customs data losses), providing a mechanism to manage project risk in the crucial area of public confidence.

Below is an overview of the Privacy Impact Assessment process derived from the Information Commissioners website:

- **Initial assessment** -Examines the project at an early stage, identifies stakeholders, makes an initial assessment of privacy risk and decides which level of assessment is necessary.
- **Full-scale PIA-**Conducts a more in-depth internal assessment of privacy risks and liabilities. Analyses privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them.
- **Small-scale PIA**-Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project
- **Privacy law compliance check**-Focuses on compliance with various "privacy" laws such as HRA, RIPA and PECR as well as DPA. Examines compliance with statutory powers, duties and prohibitions in relation to use and disclosure of personal information.
- **Data protection compliance check**-Checklist for compliance with DPA. Usually completed when the project is more fully formed.
- **Review and redo-**Sets out a timetable for reviewing actions taken as a result of a PIA and examines their effectiveness. Looks at new aspects of the project and assesses whether they should be subject to a PIA.

It is acknowledged in the Information Commissioner's Handbook that the amount of detail in a PIA can vary considerably, dependant on the system that is proposed and the extent of the privacy impact and resulting project risk. On this basis organisations are encouraged to develop a PIA process that meets their particular needs.

Privacy Impact Assessment Wales (NWIS)