PRIVACY IMPACT ASSESSMENTS

What is a Privacy Impact Assessment (PIA)?

The objective of a Privacy Impact Assessment (PIA) is to systematically identify the risks and potential effects of collecting, maintaining, and disseminating Personal Confidential Data (PCD) and help organisations comply with their Data Protection obligations.

A PIA should be considered where there is introduction of new technologies, in the commissioning of new services or where there is a change to the way that personal information is processed.

- It provides evidence that data protection risks are taken seriously within the organisation.
- It should be more efficient in use of resources to manage potential risks rather than have to address actual risks at the end of the project
- It can identify any risks to the privacy of individuals.

A PIA encourages staff to consider privacy issues, not just in projects, but across all their daily activities by reminding them of those issues and how they impact in practice.

The Information Commissioners Office (ICO) has developed a framework for organisations to use when considering a PIA and this guidance has been developed from that framework – amended specifically for health organisations.

The purpose of the template document is to provide a checklist for use in assessing data protection compliance, including a set of standard screening questions that determine whether an initial PIA is required.

Who should be involved in a PIA?

PIAs should be completed by the service lead (the person responsible for introduction or commissioning of the new service) in liaison with the Information Governance Lead (at GEM CSU) and other stakeholders from the providers of the service.

How are PIAs carried out?

Conducting a PIA does not have to be complex or time consuming and the process developed is flexible in that it can be integrated within the organisations existing approach to project management and is also scalable, depending on the scope of the project. The process of conducting a PIA should begin early in the project, but can run alongside the project development process

The PIA incorporates the following steps:

- Identify the need for a Privacy Impact Assessment – complete the screening questions
- Describe the information flows – identify what information is used, why and who it is obtained from and disclosed to.
- Identify any privacy risks – to individuals, the organisation and legal implications
- Identify privacy solutions – the IG lead will explain how any risks might be addressed
- Senior executive level sign off – report to the Senior Information Risk Owner, including an assessment of any risks or mitigating actions.

Completed PIAs should be reviewed at senior level within the organisation and if necessary an action plan developed to mitigate any identified privacy risks.

Deborah Pallant
IG Consultant Nottinghamshire

December 2013