Meeting the Requirements

Auditing

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

Auditing is an important tool for organisations in order to gain assurance that they understand and are compliant with information governance, data protection legislation and national standards. Auditing enables the proactive identification of information governance risks as well as mitigating actions to be implemented in order to address them. Auditing also allows for any mitigating controls already in place to be tested to ensure they remain effective.

Auditing provides a good opportunity to raise awareness of data protection legislation throughout the organisation. In larger organisations, such as Health Boards and Trusts with specific Information Governance teams, auditing allows the opportunity for other staff members to discuss any information governance issues or concerns, as well as enables the sharing of information governance knowledge throughout the organisation.

Organisations should carry out Information Governance audits on a regular basis to enable the organisation to demonstrate compliance with data protection legislation and national standards as well as the organisations own Information Governance Policies and Procedures. Further information on the objectives of the IG audits can be found within 'Table One'.

For the larger organisations within NHS Wales, it is recommended that Pre-Audits are forwarded and completed by Service Leads/Heads, this will enable individuals with IG responsibility to undertake to full IG Audit.

How do we reach Attainment Level 1?

The organisation should have audit processes in place to oversee the Information Governance agenda and provide assurance on their information governance responsibilities. This may include spot checks to ensure IG policies and procedures are followed and staff understand their responsibilities, information audits or data mapping exercises are carried out, through to full Information Governance Audits considering all aspects of the organisation.

Organisations should aim to identify any IG risks and implement appropriate mitigating actions for any risks identified. See 'Table Two' for further information around the suggested scope of the IG Audit. 'Table Three' details example Roles and Responsibilities for the Audit process.

How do we reach Attainment Level 2?

There should also be auditing processes in place to identify the information held by the organisation, any inappropriate use of, or access to the information. 'Table Four' sets out the ICO's expectations for internal audit programmes.

Organisations should consider using auditing tools such as 'NIIAS' or other similar clinical system audits to monitor user activity for clinical records.

How do we reach Attainment Level 3?

In addition to having auditing processes in place, the organisation should also have a process to follow up on and review any activity captured on previous audits. This may include checks to ensure that necessary adjustments, updates or ways of working have been implemented following previous identified audit finding/recommendations. The organisation should undertake regular checks to ensure the audit processes are appropriate in accordance with the processing activities.

The accountability principle is a key aspect of data protection legislation, therefore audit activity should be reported to the relevant forum, such as the Management Team, Board or Committee, to ensure appropriate oversight.

Supporting Resources

ICO: Record of Processing and Lawful Basis – *guidance on documenting your processing activities and the lawful basis*

ICO: The Accountability Framework - *Accountability is one of the key principles in data protection law*

ICO: Guide to the UK General Data Protection Regulation (GDPR)

ICO: Introduction to data protection

NHS Wales: NIIAS – *the pro-active audit monitoring system utilised in NHS Wales*

National Archives: Find out what information you have

UK GDPR – Article 30 - *Record of processing activities*

Summary Requirement

Attainment Level	Summary Requirement
1	Organisations have audit programmes in place to oversee the Information Governance agenda
2	Audit processes are used to regularly monitor appropriate use of personal information
3	There is a review process on all the auditing programmes the organisation undertakes to ensure it remains relevant and feedback is acted on