Meeting the Requirements

IG Risk Register

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

The UK General Data Protection Regulation (UK GDPR) introduced the Accountability principle, which requires organisations to take responsibility for what they do with personal data and how they comply with the other principles of the UK GDPR. Organisations must have appropriate measures and records in place to be able to demonstrate their compliance with the UK GDPR.

Article 24(1) of the UK GDPR says that:

- organisations must implement technical and organisational measures to ensure, and demonstrate, compliance with the UK GDPR;
- the measures should be risk-based and proportionate; and
- organisations need to review and update the measures as necessary.

The UK GDPR emphasises a risk-based approach to data protection. The need to identify, assess and manage privacy risks is an integral part of accountability. Understanding the risks of the way you use personal data specifically is central to creating an appropriate and proportionate privacy management framework. The organisation must be able to demonstrate that information governance risks have been identified and assessed, with mitigating measures and safeguards identified and implemented throughout the organisation. There should be a clear process in place for identifying, reporting and reviewing information governance risks.

The ICO has a number of useful resources for organisations including the page on 'Accountability and Governance'.

How do we reach Attainment Level 1?

The organisation should place high importance on minimising information risk and safeguard the interests of its patients, staff and the organisation. Information risk is inherent in all of the organisations activities and everyone working for, or on behalf of the organisation, has a responsibility to continually manage information risk. Information risk management should aim to provide the means to identify priorities and manage the risks involved in all of the organisation's activities.

Adopting an IG Risk Management Framework would be good practice with it aiming to:

- protects patients, staff and the organisation from information risks where the likelihood of occurrence and consequences are significant
- support the strategic approach to the risk management framework in which information governance risks will be identified, considered and addressed in the approval, review and control processes
- encourage pro-active rather than re-active information governance risk management

- contribute to the quality of decision making throughout the organisation by supporting robust information governance practices
- meets legal or statutory requirements
- assists in the safeguarding the organisations information assets

The organisation should routinely conduct IG risk assessments, these can be carried out in a number of ways including:

- routinely reviewing flows of personal information to ensure any information governance risks identified are mitigated
- providing clear guidance in IG risk management procedures as to the way in which IG risks and incidents are identified, assessed and managed across the organisation, and how the Information Governance Risk Register supports this process
- carrying out Data Protection Impact Assessments

The organisation should have appropriate policies, procedures and measures to identify, record and manage IG risks. See 'Table One' for the ICO's expectations on identifying, recording and managing risks.

The security principle in the UK GDPR goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just cyber security. Therefore, it is important to ensure IG risk assessments are conducted for every aspect of your processing, in some organisations this may form part of the DPIA process. However, a DPIA is only required for processing that is **likely to result in a high risk** to individuals. Further information on the DPIA process can be found within the 'Data Protection Impact Assessments' page.

How do we reach Attainment Level 2?

The organisation should have a clear process in place for the management of identified information governance risks. Where IG risks have been identified, the organisation should ensure that mitigating measures are implemented, and adopted throughout the organisation where necessary, in order to mitigate the risk. You should put appropriate action plans in place for any identified IG risks, with progress reports maintained and distributed as necessary. Considerations should be given to the lessons learnt to avoid future risk. There should also be a process in place to manage the IG Risk Register, including the addition and amendments of IG risks on the Risk Register.

All unmitigated IG risks should be reported to the appropriate forum, such as the Board or Senior Management Team, as and when required. This may be in the form of a formal reporting process or documented in the minutes of a meeting.

How do we reach Attainment Level 3?

The organisation should conduct regular reviews on the relevant processes and the IG Risk Register to ensure they remain up to date. Mitigating measures should also be tested regularly to ensure they remain effective.

The accountability principle is a key aspect of data protection legislation, therefore the organisation should have a reporting process in place to ensure any changes or actions resulting from the review of the IG Risk Register are reported to the relevant forum, such as the Board or Practice Management Team, to ensure appropriate oversight, as appropriate.

Supporting Resources

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

ICO: Data Protection by Design and by Default - *GDPR requires you to put in place appropriate technical and organisational measures*

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

ICO: Introduction to data protection

HSCIC: Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation - *This guidance document covers the reporting arrangements and describes the actions that need to be taken in terms of communication and follow up when an IG or cyber security SIRI occurs. Organisations should ensure that any existing policies for dealing with IG and cyber security SIRIs are updated to reflect these arrangement*

The National Archives: Information Assurance

The National Archives: Managing Information Risks

Summary Requirement

Attainment Level	Summary Requirement
1	The organisation analyses IG risks regularly and documents in a formal IG risk register

2	There is a clear understanding and management of the identified IG risks
3	Regular review of processes and the IG risk register are undertaken to ensure they remain up to date, with mitigations regularly checked to ensure they remain effective