Meeting the Requirements

Information Governance Management Structure

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

The UK General Data Protection Regulation 2016 (UK GDPR) includes provisions that promote accountability and governance. The new accountability principle requires the organisation to demonstrate that it complies with the principles and states explicitly that this is your responsibility as a Data Controller. The organisation will be expected to put into place comprehensive but proportionate governance measures. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the UK GDPR's emphasises their significance. See the ICO 'Overview of UK GDPR – Accountability and Governance'.

It is important that there is a consistent approach to information handling within the organisation, which complies with the law, professional standards, guidance and good practice. The ICO considers that a fundamental building block of accountability is strong leadership and oversight. This includes making sure that staff have clear responsibilities for data protection related activities at a strategic and operational level. It requires for an appropriate management structure to be adopted and that personnel are in place to oversee information governance arrangements.

Depending on the size of the organisation, such personnel may include, for example, a Head of Information Governance (IG) or Lead/Manager, a Head of Information and IT Security or Lead/Manager, a Senior Information Risk Owner (SIRO) and a Caldicott Guardian. Responsibility for assessing information handling and driving forward any required improvements would lie with one or more of these roles. Subject to the size of the organisation, one or more of these roles may be assigned to the same individual, for example, in a GP Practice the IG Lead and IT Security Lead roles may be assigned to the Practice Manager. **Note:** For the purpose of the IG toolkit, these roles are generally referred to as the IG Lead.

The Caldicott Guardian should be an existing member of the senior management team and preferably a health professional. The SIRO will be an Executive Director or other senior member of the board/management team. In general, SIROs are currently appointed in the larger NHS organisations in Wales, rather than Primary Care Service providers. The Caldicott Guardian and SIRO roles should be assigned to two separate individuals.

Under UK GDPR the organisation is required to appoint a Data Protection Officer (DPO) with appropriate qualities and expert knowledge of the law and practices. With confidentiality being a key element of the IG agenda the appointed Caldicott Guardian and DPO should work closely to ensure confidentiality of patient information. This element should be supported by adequate skills, knowledge and experience across the organisation.

See the ICO's expectations on 'Leadership and Oversight' for further guidance.

How do we reach Attainment Level 1?

There should be an organisational structure for managing data protection and information governance, which provides strong leadership, clear reporting lines and responsibilities. This requires that named individuals take responsibility for co-ordinating, publicising and monitoring standards of information handling within the organisation. The organisation should consider the responsibilities of an IG Lead and decide whether these can be met by one member of staff, or whether the role requires support from additional members of staff to a whole team. For Primary Care Service Providers there will be a written assignment of IG Lead responsibilities, for example, by adding this to existing staff job descriptions or simply a written note explaining the position.

Rather than an individual IG Lead, Health Boards and Trusts will have an Information Governance team/department in place to take responsibility for the organisation's information governance requirements. IG staff in these organisations should understand the organisational structure and their responsibilities.

In any organisation IG related job descriptions will clearly set out responsibilities and reporting lines to management and should be up to date, fit for purpose and regularly reviewed.

See 'Table One' for key responsibilities of the IG Lead within General Practice.

All organisations providing direct care to patients should appoint a Caldicott Guardian to take responsibility for confidentiality issues and seek additional advice when required. The Guardian plays a key role in ensuring that the organisation satisfies the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of the organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information.

Appointed Caldicott Guardian's may not all be the same. For example, in a health board the Guardian may be the Medical Director or Director of Nursing, whereas in a GP Practice it will be a senior partner/health professional. Regardless of the size of the organisation, they perform a key role with overall responsibility for ensuring that the management of patient information within the organisation complies with legislation, Codes of Practice and Professional Standards and will have a key working relationship with the Data protection Officer and Senior Information Risk Owner. The IG Lead/Team should have access to the Caldicott Guardian for support and advice when necessary. Further information on the role of the Caldicott Guardian can be found in the 'Caldicott Guardian Skills and Understanding' section of the website.

The Senior Information Risk Owner (SIRO) provides an essential role in ensuring that identified information security risks are followed up and incidents are managed. They will take ownership of the Information Risk Policy and associated risk management strategy and processes. Health Boards and Trusts are required to appoint a Senior Information Risk Owner (SIRO). Formal responsibility for data security should be assigned to the SIRO, and this responsibility should be detailed in the relevant individuals job role.

Note: Please see 'Table Two' for further information on the responsibilities of the Caldicott Guardian and 'Table Three' for information on the responsibilities of the Senior Information Risk Owner.

The 'UK General Data Protection Regulation 2016' (UK GDPR) introduces a duty for the organisation to appoint a 'Data Protection Officer (DPO)' or DPO as a service, due to the type of processing activities it carries out. The DPO should assist the organisation in monitoring internal compliance, inform and advise you on your data protection obligations, provide advice regarding 'Data Protection Impact Assessments (DPIAs)' and act as a contact point, where necessary, for individuals and the Information Commissioner's Office. The DPO will provide advice and support to the organisation in relation to data protection. They will support the Caldicott Guardian and IG Lead/Team to enable the organisation to adhere to legislation and standards particularly in relation to UK GDPR and the DPA. The DPO role is to advise and inform and is not accountable.

The UK GDPR says that the DPO should be appointed based on their qualities, and in particular, experience and expert knowledge of data protection law. It does not specify the precise credentials they are expected to have, but it does say that this should be proportionate to the type of processing carried out and the level of protection required for the personal information you hold. Therefore, where the processing of personal information is particularly complex or risky the knowledge and ability of the DPO should be advanced enough to provide effective oversight. It would also be an advantage for the DPO to have a good knowledge of the organisation's processes and systems, as well as its data protection needs and processing activities. See 'Table Four' or further information on the DPO.

Larger organisations, such as Health Boards and Trusts, should have an organisational IG reporting structure in place to ensure relevant information is reported through the appropriate lines. This may include Groups and Committees, as well as reporting up to the Board.

The 'Data Protection (Charges and Information) Regulation 2018' requires the organisation to pay a fee to the Information Commissioner's Office (ICO). This new data protection fee, payable every 12 months, replaces the requirement to 'notify' (or register) under previous data protection legislation. See the ICO website to 'register or renew your fee'. Failure to pay the fee will result in a fixed penalty.

Note: GMP's managed by a health board are not required to pay the data protection fee separately as their respective health board's payment will cover them. The health board's registration can be searched for on the ICO's 'Data Protection Public Register'.

How do we reach Attainment Level 2?

The Data Protection Officer, Caldicott Guardian, SIRO, Head of IG, IG Lead and any supporting staff need to be sufficiently trained to undertake their key responsibilities. Training should cover data protection legislation, security, confidentiality, appropriate information sharing and Freedom of Information Act requirements.

Note: The 'Training and Awareness' section provides further direction on training.

One of the key duties of the Information Governance Lead/Team is to develop a locally tailored IG Improvement Plan. The easiest way to create the improvement plan is by evaluating your current

attainment levels in the Welsh IG Toolkit and then to set targets for improvement against each 'Requirement'. Setting targets and entering comments within each assessment of the IG Toolkit will help you to develop/update your improvement plan. See 'Table Five' for developing an Improvement Plan.

The improvement plan should be challenging but realistic and needs to be agreed with the Senior Management Team so that adequate time, attention, and where necessary, resources are available to complete the work. The Data Protection Officer will be available to provide advice on areas of concern identified by the improvement plan, to enable the organisation to comply with data protection legislation.

How do we reach Attainment Level 3?

Effective Information Governance is not something that is self-sustaining; there needs to be sufficient managerial attention paid to ensure that:

- plans to address those areas requiring improvement are put in place;
- identified improvements are delivered;
- staff are trained on any relevant areas.

Regular consideration of information governance arrangements are required by the Senior Management Team and Data Protection Officer, providing either intervention where necessary or agreement that the arrangements are satisfactory. Arrangements should be reviewed at least bi-annually; more frequently where there are concerns or where there has been an incident. The Data Protection Officer should be able to assure the Senior Management Team that the organisation is not carrying more risk than they are comfortable with, and that there are processes in place to help mitigate this risk.

Supporting Resources

Template IG Improvement Plan Health Boards and Trusts - *To provide organisations/practices with an accessible improvement plan to list identified IG areas for improvement following the completion of the IG toolkit.*

Template IG Improvement Plan GMPs - *To provide organisations/practices with an accessible improvement plan to list identified IG areas for improvement following the completion of the IG toolkit.*

Exemplar GMP IG Improvement Plan - *An example of an Improvement Plan populated by Practice Managers in the BCU locality*

All Wales Information Governance Policy

All Wales Internet Use Policy

All Wales Email Use Policy

All Wales Information Security Policy

All Wales Information Governance Policy for Primary Care Service Providers

All Wales Internet Use Policy for Primary Care Service Providers

All Wales Email Use Policy for Primary Care Service Providers

All Wales Information Security Policy for Primary Care Service Providers

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

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

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

ICO: Introduction to data protection

NHS Digital: Data Security and Information Governance - *NHS Digital [England] offers guidance on protecting data and handling information securely*

The UK Caldicott Guardian Council (UKCGC) - *The UKs national body for Caldicott Guardians*

UKCGC: A Manual for Caldicott Guardians - *A manual of good practice for Caldicott Guardians, setting out what Guardians should do, what their powers are, key legislation and working relationships, etc.*

GOV.UK Information: To Share or not to share? The Information Governance Review (2013) - *An independent review of how information about patients is shared across the health and care system*

Summary Requirement

Attainment Level	Summary Requirement
1	Responsibility for driving improved information governance has been assigned to appropriate individuals within the organisation. This forms part of their job description and daily duties
2	Responsible individuals have received appropriate training to take ownership of the information governance agenda and identified improvements from previous IG Toolkit submissions. These have formally been documented to form an IG Improvement/Action Plan

3	The IG arrangements and progress against the IG Improvement/Action Plan are reviewed by the IG Lead and DPO, and is reported to the relevant forum on a regular basis