Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit

IGDC • DHCW

Expectations Guidance Document

1.1 - Leadership and Oversight

Introduction

This guidance will provide basic information on what will be required from Organisation Administrators and Users to work through and complete the Leadership and Oversight section of the Welsh Information Governance Toolkit (WIGTK).

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. Some organisations are legally required to appoint a Data Protection Officer (DPO); but everyone must allocate sufficient resources and make sure that data protection is a shared responsibility, rather than solely the task of someone working directly in a data protection role, to ensure the organisation can meet its data protection responsibilities.

You will need to consider if the organisation has an appropriate organisational structure in place for information governance and data protection, with appropriate staff appointed to the required positions.

Minimum Expectations

Information Governance Responsibilities

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.

Whilst IG and data protection is everybody's responsibility, there must be a named person within your organisation who takes overall, senior responsibility for IG and data protection issues. Their responsibility is to provide senior level leadership and guidance. For example, Caldicott Guardian or IG Lead.

The IG Lead is not required to carry out all the work necessary to meet the NHS IG requirements, but should be able to co-ordinate the activities of staff given data protection legislation, confidentiality, information sharing, Freedom of Information Act and Environmental Information Regulations responsibilities, monitor the organisation's information handling and sharing activities to ensure compliance with the law and ensure that all staff are sufficiently trained in IG to support their role.

Reporting lines and overall responsibility for IG

A fundamental building block of accountability is strong leadership and oversight. The ICO expects the senior management team or Board to have overall responsibility for IG and data protection.

The organisation should document the roles with responsibilities for IG and data protection within an organisational structure, with clear reporting lines outlined. The evidence uploaded should show the Organisational structure including job descriptions.

If your Organisation has groups or committees set up, the oversight group should consist of key staff, e.g. the DPO, who regularly attends group meetings.

Please note, the following part is only applicable to HBs/SHAs/Trusts:

Depending on the organisation size and structure, it may be appropriate to establish an IG forum, group, or committee. These groups should meet the following criteria:

- Is chaired by appropriate senior staff members, e.g. the DPO or SIRO
- Describes it's aims in clear terms of reference
- Maintains a record of meeting minutes.
- Covers a full range of data protection related topic.
- Has a work or action plan that is regularly monitored
- Reports to the senior management team or board on IG and data protection issues and risks

Example evidence could be either terms of reference for a group/forum or committee, minutes from appropriate meetings, extract from Board papers, or a policy document.

Improvements plans - HBs/SHAs/Trusts only

The organisation's IG Action Plan or Improvement Plan will demonstrate that targets, resulting from previous assessments, are collated to track and record ongoing improvement of IG compliance throughout the organisation. Example evidence would be an action plan/improvement plan.

Appointment of a Data Protection Officer (DPO)

Under the UK GDPR, you must appoint a Data Protection Officer (DPO) if:

- you are a public authority or body (except for courts acting in their judicial capacity),
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking), or
- your core activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offences.

The appointed DPO must fulfil the requirements set out in UK data protection legislation, including, having expert knowledge of data protection law and practices. The DPO must be adequately supported and provided with sufficient resources to perform their role. The DPO should report directly to senior management and must be given the required independence to perform their tasks.

The tasks of the DPO include:

- Providing advice and guidance on the organisations data protection obligations,
- Monitoring compliance with data protection legislation,
- Raising awareness and training,
- Advise on Data Protection Impact Assessments (DPIAs),
- Liaise with the Information Commissioner's Office (ICO).

The organisation should ensure that both staff and the public are informed of who the DPO is and how to contact them.

Appointment of a Senior Information Risk Owner (SIRO) - HBs/SHAs/Trusts only

The Senior Information Risk Owner (SIRO) provides a focal point for managing information assets, risks, and incidents. Formal responsibility for data security will be assigned to the SIRO.

Currently, only Health Boards, Trusts, and SHAs are required to appoint a SIRO, however other organisations may also choose to appoint someone to this role.

The SIRO must be of an appropriately senior level, such as an Executive Director or other senior board member. The SIRO should be part of the organisation's management hierarchy and understand how the organisation's strategic business goals may be impacted by information risks. They will form part of the oversight group as well.

Responsibilities of the SIRO include:

- To develop and implement an IG Information Risk Policy that is appropriate to all departments of the organisation and their uses of information setting out how compliance will be monitored.
- To act as the central point for information risk assessments ensuring that management policies, management methods and standards are documented and maintained consistently.
- Owning the organisation's information incident management framework.

Appointment of a Caldicott Guardian

In December 1997 the Department of Health, Caldicott Committee Report on the Review of Patient-Identifiable Information made the initial recommendation of:

"A senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information".

The role of the Caldicott Guardian was mandated in NHS Wales in the 'WHC (99) 92 Protecting Patient Identifiable Information: Caldicott Guardians in the NHS'.

The Caldicott Guardian will oversee the Organisation's compliance in relation to the 'Caldicott Principles'.

Responsibilities of the Caldicott Guardian include:

- Information sharing - The Caldicott Guardian should oversee all arrangements, protocols, and procedures where confidential personal information may be shared with external bodies and others with responsibilities for social care and safeguarding. Staff should be advised to seek assistance from the Caldicott Guardian where necessary for such things as a request from the police for access to people's information, requests from a patient to delete their records and an actual or alleged breach of confidentiality.
- Internal processing - The Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- Confidentiality and data protection expertise - the Caldicott Guardian should develop a strong knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott and information governance functions, but also on external sources of advice and guidance where available.
- Oversee the organisation's compliance with the 'Caldicott Principles'
- Play a key role in ensuring that the organisation satisfies the highest practical standards for handling individual's personal health and care information
- Advise on options for lawful and ethical processing of individual's health and care information
- Actively support work to facilitate and enable information sharing
- Ensure that current policies and procedures are in place which impact upon the accuracy, management, confidentiality, sharing and retention of health and care records
- Instigate regular management audits to inform future work

Please see more on the Caldicott Guardian role here: Caldicott Guardian role — UKCGC

Operational IG Responsibilities - HBs/SHAs/Trusts only

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.

Operational roles should be assigned to support the practical implementation of IG and data protection throughout the organisation. Staff with operational responsibility must have the authority, support and resources to carry out their duties effectively. Job descriptions should clearly set out their duties and responsibilities, along with reporting lines to management.

Being responsible for compliance with IG and data protection requires organisations to create a positive culture of commitment towards data protection. One of the ways you can do this is to ensure staff have a good level of understanding, awareness and know who to approach for support and who can answer any queries. The organisation should promote the contact details of relevant IG colleagues to all staff, setting out who may be best placed to provide support.

FOI and EIR Support - HBs/SHAs/Trusts only

The organisation should have an established process for the management of its Freedom of Information (FOI) & Environmental Information Regulations (EIR) responsibilities.

Organisations should have specific staff responsible for processing FOI requests. The FOI Officer will be responsible for:

- Acknowledging and responding to FOI requests.
- Logging and updating cases in our case management system.
- Liaising with key colleagues to obtain answers to FOIs requests.

For further details, please see the ICO's Guide to Freedom of Information

Information Commissioners Office (ICO) Registration

Every organisation who processes personal data needs to pay a registration fee to the ICO unless the organisation is exempt. More information on the data protection fee can be found on the ICO website.

The organisation must renew their registration and pay the data protection fee each year. You are required to provide certain information to the ICO, and you must ensure these details are kept up to date. This includes your:

- Organisation address
- Contact details (name, job title, address, email, and phone number) of the person who has been selected to receive correspondence for the organisation.
- Data Protection Officer's details (including adding a DPO)
- Trading names (other names by which the organisation may be known)
- Payment tier

You can search the Register of Fee Payers on the ICO website to review your details.

Your organisation can use the ICO online service to change, add, or update the details held about your registration.

Exceeded Expectations

This section is not required to be completed; however, it will help to further demonstrate your compliance and provide assurance.

These questions build on those you will have answered in the minimum expectations section; however, they are slightly more in depth.

Please note: If you are a GP or Community Pharmacy completing the IG Toolkit, there are no exceeded expectations to be completed for this section.

Reporting of IG Information

The organisation should have an effective process in place to ensure senior management or board are provided with regular updates on a variety of IG matters, including:

- training compliance
- compliance in responding to individual rights requests
- FOI & EIR compliance
- IG Risks
- data breaches, near misses, patterns noted
- audit findings
- DPIA figures

These updates should take place at least quarterly, in addition to ad-hoc reports as needed.

Example of evidence would be copy of board papers or escalation reports.

Promoting a Positive IG Culture

A just culture is a well-established concept in safety related fields, where trust and engagement are vital components in ensuring that any incidents are learnt from and not repeated.

This attitude can be replicated in IG through a positive IG culture. Not just when an incident has occurred, but in any situation where understanding exactly what is happening is required. A positive culture gives people confidence that not only can they speak openly and see the organisation improving as a result, but that any actions or decisions will be reviewed fairly.

Communication and consistency are key in facilitating a positive culture towards IG.

Decision-makers, such as Board Members and Directors promote a proactive, positive culture of data protection compliance. This can be done through a variety of methods such as blogs published on the organisation's website or intranet page, presentations in staff briefings or conferences, or email communications. Example of evidence can be copies of emails, blogs, or other communications.