Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit

IGDC • DHCW

Expectations Guidance Document

1.3-Training and Awareness

Introduction

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

To ensure organisational compliance in line with current legislation and relevant guidance relating to Information Governance (IG), staff must receive appropriate training. Therefore, IG training should be made mandatory for all staff, comparable to health and safety training. IG training needs for all staff members should be routinely assessed, monitored, and adequately provided, based on their specific roles.

Information Governance knowledge and awareness should be at the core of an organisation's objectives, embedded alongside other governance initiatives and should provide a stable foundation for the workforce. This will make sure that all employees receive appropriate training and understand what it required of them and what responsibilities they have. The training must be relevant, accurate and up to date. Without this knowledge, the ability of the organisation to meet its legal and policy requirements will be severely impaired.

Minimum Expectations

Training Needs Analysis (TNA)

The organisation should conduct a Training Needs Analysis that includes training for all staff on key areas of data protection, such as handling requests for information, data sharing, information security, personal data breaches and records management. The training must be relevant, accurate and up to date.

The TNA should include staff receiving induction and refresher training, regardless of how long they will be working for your organisation, their contractual status or grade.

The ICO expects there to be an all-staff data protection and information governance training programme in place. The training needs of all staff should be considered when creating the programme, including those who are unable to access traditional training methods such as eLearning through to those in specialist roles who require additional training.

The organisation's TNA should include all individuals working for or on behalf of the organisation. This includes:

- Staff members
- GPs and GP Partners
- Directors/ Trustees
- Locums
- Agency workers
- Students
- Trainees

- Secondees
- Volunteers
- Contracted third parties

All individuals should receive induction training prior to accessing personal data and at least within one month of their start date.

The organisation's TNA should be reviewed and updated every year as a minimum. In addition to regular reviews, the training plan should be updated to reflect any:

- Changes to the organisation's structure or processes
- Changes to legislation

Training Log/Register

It is important to retain records of staff training. This is often done using a log or register.

The record should include the date training was completed, what course was attended and what training materials were used, for example All Wales eLearning package V5.0.

As well as demonstrating the organisation's overall IG training compliance, the organisation may need to rely on these records to evidence training was provided and what this included, should an incident involving a staff member occur.

Requirements to complete training

All staff within NHS Wales are required to undertake mandatory IG training on commencement of their employment, and at least within one month of their start date. Following this refresher training must be undertaken every two years.

All staff includes:

- Staff members
- GPs and GP Partners
- Directors/ Trustees
- Locums
- Agency workers
- Students
- Trainees
- Secondees
- Volunteers
- Contracted third parties

Your organisation must be able to demonstrate that at least 75% of all staff throughout the organisation have completed IG mandatory training in the last two years.

The organisation should ensure that staff training includes a form of knowledge check such as a multiple-choice test or quiz to verify staff understood the training they have attended.

It is also important that staff can provide feedback on the training they receive. This will help the organisation to deliver effective training sessions that meet the needs of all staff members.

The organisation should also ensure that staff training is easily accessible to all members of staff, including those with limited computer access and those working various shift patterns. Your organisation should be able to evidence that it uses a variety of appropriate methods to raise staff awareness around training and the profile of data protection and information governance. For example, by using emails, team briefings and meetings, posters, handouts, and staff intranet.

Further guidance on monitoring understanding and awareness raising can be found in the ICO's Accountability Framework.

Low Levels of Training Compliance

The organisation should monitor staff training compliance across various levels, such as directorate or department, to identify any patterns of low compliance.

Compliance levels that fall below the agreed baseline of 75% for GPs and Community Pharmacies or 85% for Health Boards, Trusts, and Special Health Authorities, should be targeted for intervention. This may include intervention and a high-level push at director level, or targeted training sessions aimed at specific teams or staff groups.

It is important to monitor when staff do not attend training sessions and that you take steps to follow up with staff who do not complete the training.

Appropriate Training for Staff

The ICO expects specialised roles or functions with key data protection responsibilities receive additional training and professional development beyond the basic level provided to all staff.

It should be detailed in your organisations TNA that staff with information governance and data protection responsibilities require additional and specific training to their individual responsibilities. It is important that your organisation details the training and skills requirements in job descriptions.

Further guidance relating to training for specialised roles can be found in the ICO's Accountability Framework.

Data Protection Officer (DPO)

The UK GDPR states that all public authorities must appoint a data protection officer. The DPO must possess the appropriate professional qualities, including an expert knowledge of data protection law and practices. Your organisation must provide the DPO with the appropriate resources and access to maintain their professional knowledge.

This may be demonstrated through the achievement of professional data protection qualifications such as BCS Practitioner Certificate in Data Protection, along with the completion of continuous professional development activities.

Please see ICO Guidance for details on the expected professional qualities a DPO should possess.

Caldicott Guardian

The Caldicott Guardian must undertake specialist training above the basic level for all staff to enable them to conduct their role effectively. In addition, continuous professional development activities in the field of information governance should be undertaken. This may include attendance at formal Caldicott Guardian courses or workshops, attendance at Caldicott Guardian Council meetings, or attending of IG related training courses.

The Information Governance Review (2013) concluded that "in addition to the standard training and education, Caldicott Guardians should demonstrate continuous professional development in information governance on an annual basis".

The Manual for Caldicott Guardians (2017) provides guidance on Learning and Development for Caldicott Guardians.

The Caldicott Manual has since been updated and is available on The UK Caldicott Guardian Councils website.

Senior Information Risk Owner – HB/SHAs/Trusts only

The Senior Information Risk Owner must undertake training above the basic level for all staff to enable them to conduct their role effectively and take overall responsibility for the organisation's information risks. This may include formal SIRO training courses, or other relevant training courses for example, information security or information risk.

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.

Managing, approving, and delivering training – HB/SHAs/Trusts only

The organisation should ensure they have suitably qualified staff in the relevant subject matter who are available to deliver the training outlined in the organisation's training plan.

Having a subject matter expert manage, approve, and deliver the training will ensure the content is accurate and up to date in line with current legislation.

Evidence of Training Awareness

The organisation should use a variety of appropriate methods to raise staff awareness and the profile of data protection and information governance. For example, by emails, team briefings and meetings, posters, handouts, and blogs.

It is important that all members of staff are taken into consideration when advertising training to ensure that it is accessible to everyone e.g., not just advertised electronically as staff may not access computers on a regular basis.

85% Training Compliance – GPs and CPs only

The organisation should be able to demonstrate that at least 85% of staff throughout the organisation have completed IG mandatory training in the last two years. The ICO expects the training programme to include induction and refresher training for all staff on data protection and information governance.

This includes conducting an assessment at the end of the training to evaluate staff understanding and make sure that it is effective.

It is important to remember the requirement for induction and refresher training to be undertaken by for all staff, no matter what their level. By ensuring this is regularly reviewed, it will help to maintain this level of training compliance.

95% Training Compliance – HB/SHAs/Trusts only

The organisation should be able to demonstrate that at least 95% of staff throughout the organisation have completed IG mandatory training in the last two years. The ICO expects the training programme to include induction and refresher training for all staff on data protection and information governance.

This includes conducting an assessment at the end of the training to evaluate staff understanding and make sure that it is effective.

It is important to remember the requirement for induction and refresher training to be undertaken by for all staff, no matter what their level. By ensuring this is regularly reviewed, it will help to maintain this level of training compliance.

Regular reporting of training compliance – HB/SHAs/Trusts only

The board, or highest senior management level, has the overall responsibility for data protection and information governance training compliance.

The organisation should have an effective process in place to ensure that senior management are provided with regular updates on a variety of IG matters, including training compliance. This could be in the form of reports broken down by various levels, such as directorate or department, or having regular meetings to discuss such matters.