Meeting the Requirements

Physical Security Measures

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

Article 5 of the UK General Data Protection Regulation (UK GDPR) concerns the 'integrity and confidentiality' of personal information. It says that personal data shall be:

"Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"

This means that the organisation should have appropriate technical and organisational security measures in place to prevent personal information that it holds from being deliberately or accidentally compromised. The organisation should ensure an 'appropriate' level of security is in place 'appropriate' to the risk presented by its processing. Whilst information security is sometimes considered as cybersecurity (the protection of your networks and systems from attack), it also covers other things such as **organisational or physical security measures**.

Organisations must ensure that physical security measures are in place to protect not only personal information but to also ensure the security of hardware and software. It is likely that there may already be established security procedures in place however, these procedures need to be regularly reviewed and made available to staff. See 'Table One' for the ICO's expectations on secure physical locations.

The ICO provides more detailed and useful advice on Information Security in its 'Guide to the UK GDPR'. There must be measures in place to delay and prevent unauthorised access, to detect attempted or actual unauthorised access, and to ensure that there are procedures for staff to follow in the event that unauthorised access does occur. The protection provided to premises should be balanced against the identified risks; there should be an assessment of whether a particular risk is likely to occur, and appropriate measures put in place to minimise that risk. See 'Table Two' for the ICO's expectations on unauthorised access.

If all staff members take responsibility in actively contributing towards creating a safe and secure environment for all those who use the organisation, it will assist in protecting:

- individuals' confidentiality
- the property and its content against loss, fraud, malicious acts, damage and trespass
- from criminal offences which breach security

Formal user access provisions should be defined, this should include access for all staff, including temporary staff, and third-party contractors to all relevant locations, systems and services required to fulfil their role, for example, new starter process. Regular reviews of users' access rights should be in place and adjusted accordingly, for example, when an employee changes role or leaves the organisation.

If and when there is a business need to store personal data on removeable media, you should minimise the personal information and the organisation should implement a software solution that can set permissions or restrictions for individual devices as well as an entire class or devices.

You should not allow staff to take equipment, information or software off-site without prior authorisation. The organisation should maintain a log of all mobile devices and removeable media used and who they are allocated to.

How do we reach Attainment Level 1?

Responsibility for security of IT and the premises should be appointed to appropriately placed individuals within the organisation. All other staff, whether they are clinical or administrative, must receive appropriate training so that they are aware of their responsibilities regarding security.

Organisations should have procedures in place for staff to follow which are easily available. These should support staff in knowing when to challenge unidentified visitors in controlled areas, to know how to check that windows, doors and blinds are closed every evening and in supervising collections/deliveries etc. The organisation should hold a record of all individuals with access to restricted areas and ensure there is a process in place for controlling staff access for new starters, movers and leavers.

The principle of 'least privilege' must be applied, so that users do not have access to information that they have no business need to see. Staff should not accumulate system access over time. User privileges should be proactively managed so that there is, as far as is practicable, a forensic trail back to a specific user or user group. Where necessary the organisation will look to non-technical means of recording IT usage, for example, sign in sheets, CCTV, correlation with other systems, shift rosters etc.

There should be a staff register / repository of current staff and their roles. The register should be up to date and reflect when staff are recruited, their change of role(s) or if they leave the organisation. Managing access should be a continuous process.

How do we reach Attainment Level 2?

Staff will play a key role in ensuring the organisation is secure for fellow colleagues and patients by following the procedures in place to prevent unauthorised access to the organisation.

Staff should be made aware of measures that are put in place should an event where unauthorised access occur, for example, not to enter the premises alone where there is evidence of a break-in as the intruder may still be inside. Staff should also be made aware of who to notify and where possible minimise any potential losses. The organisation should ensure staff are aware and actively encouraged to maintain security measures in their own department and training provided as necessary.

How do we reach Attainment Level 3?

Routine security audits should be conducted to ensure compliance with physical security measures. An action plan should be developed having identified any areas of risk; the risks should be weighed against the likelihood of the threatened risk actually occurring. For example, the assessment may identify a risk of unauthorised access; the question to be asked is whether this is a

high, medium or low risk. Where the risk of a breach in security is likely, the necessary resources should be allocated to increase the physical security of those assets. In the example above this may require installing key-code locks to minimise the risk of an unauthorised entry. However, where the perceived risk is low, it may be decided that action is unnecessary at this time; but this should be documented, and the area kept under regular review. All physical security improvements identified in checks/audits should be fully implemented or escalated appropriately.

Following each security audit consideration should be given to updating the guidance / procedures to reflect any new ways of working or to highlight the purchase of new equipment, this should be shared with all staff and regularly reported to the relevant Board/Committee. There should be checks in place to ensure that staff members comply with the procedures. Awareness and training should be provided to all new staff as part of their induction, and existing staff should be provided with regular updates as necessary.

It is important that any new security measures are subject to regular risk assessment. Consideration should also be given to suppliers to the organisation, to ensure that they too adhere to this requirement.

Supporting Resources

All Wales Information Security Policy – *Developed for Health Boards and Trusts in NHS Wales by the Information Governance Management Advisory Group (IGMAG) and forms part of the IG Framework in NHS Wales*

All Wales Information Security Policy for Primary Care Service Providers - *The policy is supplementary to the All Wales policy for Health Boards and Trusts and forms part of the IG Framework for NHS Wales*

All Wales Information Governance Policy- *Developed for Health Boards and Trusts in NHS Wales by the Information Governance Management Advisory Group (IGMAG) and forms part of the IG Framework in NHS Wales*

All Wales Information Governance Policy for Primary Care Service Providers - *The policy is supplementary to the All Wales policy for Health Boards and Trusts and forms part of the IG Framework for NHS Wales*

ICO: Guide to Security

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

Confidentiality: Code of Practice for Health and Social Care in Wales - *This document sets out non-statutory guidance on best practice for those who work within or under contract to NHS or local authority social services authorities operating in Wales concerning confidentiality and the consent of patient and social care service users to the use of their health and social care records.*

General Medical Council - Confidentiality: Good Practice in Handling Patient Information 2018 - *Confidentiality (2018) sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow. Supplementary guidance explaining how these principles apply in situations doctors often encounter or find hard to deal with is also available*

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

Summary Requirement

Attainment Level	Summary Requirement
1	The organisation holds a set of policies and procedures addressing the security of all premises and departmental areas
2	Improvements identified by the risk assessment are being made to secure the premises, equipment, records and other assets including staff. Staff are aware of and encouraged to maintain security measures
3	All reasonable steps have been taken to ensure the premises is secure by undertaking regular checks/audits and any improvements are considered and implemented where necessary. Supplementary policies and procedures are regularly reviewed and approved