Meeting the Requirements

Technical Security Measures

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

Senior Management must actively support information security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.

A key principle of the UK GDPR is that personal data is processed securely, by means of 'appropriate technical and organisational measures'. This is the 'security principle'. The measures adopted must be appropriate to both the circumstances and the risk your processing poses. Your measures must ensure the 'confidentiality, integrity and availability' of the systems, services and the personal data you process'.

Confidentiality ensuring you can only view what you need, to administer the system and not disclose sensitive information

Availability ensuring that systems are accessible when required and all maintenance is agreed to local standards

Integrity ensuring you do not alter records inappropriately

Information Security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help the organisation to demonstrate compliance with other aspects of the UK GDPR.

The ICO provides more detailed and useful advice on Information Security in its 'Guide to the UK GDPR'.

How do we reach Attainment Level 1?

An Information Security policy, approved by Senior Management must be in place, published and communicated to all employees and relevant external parties. The policy will enable the organisation to demonstrate how you are taking steps to comply with the security principles of the UK General Data Protection Regulation (UK GDPR). Policies and procedures should set out how staff access technical systems that process personal data is managed. A 'NHS Wales Information Security Policy for Primary Care Service Providers' is available for organisations to adopt if they wish.

The 'NHS Wales Email Use Policy for Primary Care Providers' must be adopted by each organisation who make use of the NHS Wales Email Service. The organisation must ensure that all staff are aware of the policy and understand their responsibilities in complying with the requirements of the policy.

The organisation must ensure that the 'NHS Wales Microsoft 365 Acceptable Use Policy for General Medical Practitioners' is implemented and that all staff are aware of the policy and understand their responsibilities. The policy sets out responsibilities when staff access the applications, including email via Outlook, through their NHS Wales Office 365 account.

A suite of All Wales Policies have been developed for primary care service providers to adopt for the Practice. Staff should be encouraged to confirm they have read and understand these policies, if adopted. The full list of All Wales Policies for primary care service providers can be found on the 'Policies and Procedures' page of the IG website.

Access to personal data should be limited to authorised staff only and regular review of users' access rights should be in place. It is recommended for organisations to have an Access Control policy established which specifies that users must follow your practices in the use of secret authentication information, for example, passwords or tokens.

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. An important factor is to have access, based upon what staff need for their role today, not what role they previously had or what role they may do in future.

Privileged access rights should be restricted and controlled with a log of user access to systems holding personal data. Regular reviews of users' access rights should be in place and adjusted accordingly, for example, when an employee changes role or leaves the organisation. See 'Table One' for the ICO's expectations on preventing unauthorised access to systems and applications.

The organisation should have appropriate mechanisms in place to manage the security risks of using mobile devices, home or remote working and removable media. The organisation is expected to have a Mobile Device and Remote Working Policy in place which can demonstrate how the organisation will manage the associated security risks.

Processes should be in place to avoid unauthorised access to or disclosure of the information processed by mobile devices, for example, encryption and remote wiping capabilities. Security measures should be implemented to protect information processed when home or remote working, for example, VPN or two-factor authentication.

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.

Poor information security leaves the organisation's systems and services at risk and may cause real harm and distress to individuals; in some extreme cases lives may even be endangered.

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.

How do we reach Attainment Level 2?

For each system there should be an understanding of what events are monitored and how. This monitoring should be recorded against each system holding personal information. If the organisation has an established and well-regarded information asset register, this information can be amended to that asset record. The organisation will also need to ensure that it has appropriate processes in place to test the effectiveness of the measures and undertake any required improvements.

Staff should be made aware and understand that there is capability for their actions within systems to be monitored and recorded. With the sensitivity of the systems in the organisation, the monitoring should be granular and extensive. Greater staff awareness that their actions are monitored within systems can have a positive effect on reducing the more dubious actions some staff can take within systems. It is important that staff are reminded of monitoring, it can be a discreet event or part of a wider employee induction. All staff should understand what constitutes deliberate, negligent or complacent behaviour and the implications for their employment. Insecure behaviours are reported without fear of recrimination and procedures, which prompt insecure workarounds to be reported with action taken.

System administrators do not have the same level of role limited protection, so it falls to the individual. System administrators therefore have a great deal of system power and with great power comes great responsibility. The system administrator needs the highest level of trust in terms of respect of the confidentiality, integrity or availability of the systems they support.

The organisation has a responsibility to ensure individuals behaviour is as expected when accessing systems containing personal data. Therefore, auditing activity, such as the use of NIIAS, should be routinely monitored.

Bring Your Own Device (BYOD) raises a number of data protection concerns due to the fact that the device is owned by the user rather than the 'Controller'. It is crucial that the Controller ensures that all processing, for personal information which is under his control, remains in compliance with data protection legislation. Protecting information in the event of loss or theft of the device will need to be considered but not to the exclusion of other risks. Controllers must also remain mindful of the personal usage of such devices. Technical and organisational measures used to protect personal information must remain proportional to and justified by the real benefits that will be delivered.

There should be a BYOD policy implemented within the organisation. The ICO are currently updating its guidance on this subject, the current version is available on the 'ICO website'.

How do we reach Attainment Level 3?

Routine technical security audits should be conducted to ensure compliance with technical security measures. All technical 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, this should be shared with all staff and regularly reported to the relevant forum i.e. Management Team/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.

Supporting Resources

All Wales Email Use Policy for Primary Care Service Providers - *The policy is supplementary to the All Wales policy for Heath Boards and Trusts and forms part of the IG Framework in NHS Wales. The organisation must ensure this national policy is implemented and that all staff are aware of the policy and understand their responsibilities in complying with the requirements of the policy*

NHS Wales Microsoft 365 Acceptable Use Policy for General Medical Practitioners - *The AUP sets out staff responsibilities when accessing the applications, including email via Outlook, through their NHS Wales Office 365 account. The organisation must ensure this national policy is implemented and that all staff are aware of the policy and understand their responsibilities in complying with the requirements of the policy*

All Wales Internet Use 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. The organisation must ensure this national policy is implemented and that all staff are aware of the policy and understand their responsibilities in complying with the requirements of the policy*

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. The policy is available for organisations to adopt as best practice, rather than developing their own, is they wish*

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. The policy is available for organisations to adopt as best practice, rather than developing their own, is they wish*

All Wales Email Use 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 for NHS Wales*

All Wales Internet Use 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 - *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 - *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*

ICO: Guide to Security

ICO: Bring Your Own Device – *This guidance has not been updated since the implementation of the UK GDPR and DPA 2019 however, the guidance is still relevant*

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

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

ICO: Introduction to data protection

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

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*

NHS Wales: Secure File Sharing Portal (Move-It)

A list of TLS e-mail enabled organisations *(Internal only)* - *This is a list of organisations external who have enabled TLS (Transport Layer Security) on their e-mail addresses.*

Summary Requirement

Attainment Level	Summary Requirement
1	The organisation holds a set of policies and procedures addressing the technical measures to protect inappropriate access to personal data
2	Staff are informed that access to IT systems is monitored
3	All reasonable steps have been taken to ensure technical measures provide sufficient security by undertaking regular checks/audits. Any improvements are considered and implemented where necessary