Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit

IGDC • DHCW

Summary of Changes

Welsh IG Toolkit Question Set 2026/27

Health Boards, Trusts, SHAs

Introduction

This document outlines the proposed changes to be made to the Welsh Information Governance Toolkit (WIGTK) question set for submission in 2026/2027.

There are minimal changes planned, proposed changes are a result of feedback received as part of the stakeholder question set consultation process, recent changes in legislation in relation to the Data Use and Access Act 2025, considerations around the use of AI and maintaining equivalency with NHS England's Data Security and Protection Toolkit (DSPT).

In summary:

- A total of 7 additional questions have been added to the question set.
- One question has been reworded, there is no change to the requirements of this question and previous answers and evidence will be carried over.
- An amendment has been made the tooltip for two questions

Additional Questions Added

1.2 Policies and Procedures

'Does the organisation have a process or policy statement around the use of Artificial Intelligence (AI)?'

1.4 Individual Rights

'Does the organisation have a process for handling data protection complaints which includes:

- A way of making data protection complaints to the organisation
- The requirement to acknowledge receipt of complaints within 30 days of receiving them
- Ensuring that appropriate steps and enquiries are made to respond to individuals without undue delay
- Inform individuals of the progress and outcome of their complaints without undue delay.'

1.5 Records of Processing and Information Assets

'Does the organisation have an up to date asset register in place which details all hardware, software and information assets?'

1.7 Risks and DPIAs

'If the organisation utilises Artificial Intelligence (AI) technologies, has an appropriate DPIA been completed for each solution?'

'If the organisation uses ambient voice technologies, does the solution in place meet the requirements set out in the relevant Welsh Health Circular (WHC/2025/026)?'

3 Information Security

Current Question – Minimum Expectation (IS-ME-5): *'Has the organisation submitted a CAF Self-Assessment within the previous 18 months?':*

A follow-up question has been added to the WIGTK question set following feedback during the consultation process.

'Please confirm the date the organisation last submitted their CAF Self-Assessment?'

4 Video Surveillance

'Does your organisation utilise a video surveillance system?'

Questions Reworded

3 Information Security

Current Question – Minimum Expectation (IS-ME-9): *'Are the IT systems and the software used in the organisation:*

** supported by the manufacturer and the latest updates installed*

** no longer supported by the manufacturer, however the risks are understood and managed for these systems/software and have been reported to the Board or senior management team*

** it is unknown if systems and software remain supported by the manufacturer and the latest updates are installed'*

Question reworded for 26/27: 'Are the IT systems and the software used in the organisation:

* supported by the manufacturer and the latest updates installed **promptly**

* no longer supported by the manufacturer, however the risks are understood and managed for these systems/software and have been reported to the Board or senior management team

* it is unknown if systems and software remain supported by the manufacturer and the latest updates are installed'

Changes to Tooltip Information

3 Information Security

Current Tooltip – Minimum Expectations (IS-ME-5): *The NIS Regulations provides legal measures to ensure both cyber and physical resilience of networks and information systems are in place for operators of essential services.*

NHS Health Boards/ NHS Trusts and Special Health Authorities are considered operators of essential services and are required to meet the requirements of the NIS Regulations.

Organisations should have in place appropriate and proportionate security measures to manage risks to the network and information systems that support their services, in line with the Welsh Government's Network and Information Systems Regulations 2018 guidance.

In Wales the NHS Wales Cyber Resilience Unit (CRU) is the appointed competent Authority for the NIS regulations within healthcare in Wales and requires the Cyber Assessment Framework assessment to be completed.

Updated Tooltip for 26/27: The NIS Regulations provide legal measures to ensure both cyber and physical resilience of networks and information systems are in place for Operators of Essential Services (OES).

NHS Health Boards/ NHS Trusts and Special Health Authorities are considered OES under the NIS Regulations and are therefore required to meet its requirements.

Organisations should have appropriate and proportionate security measures in place to manage risks to the network and information systems that support their services, in line with the Welsh Government's Network and Information Systems Regulations 2018 guidance

5 Business Continuity

Current Tooltip – Minimum Expectations (BC-ME-3): *'It is recommended that BCPs and disaster recovery plans are regularly tested.*

Table top exercises or simulations that include a cyber-scenario (such as hacking) should be used to test that the BCP is fit for purpose.'

BC-ME-3 asks organisations to confirm when the business continuity plan (BCP) was last tested. It was raised that users found it difficult to provide specific information for this as there was uncertainty surrounding what classes as testing the BCP. Therefore, the tooltip to assist users has been updated to include more examples of scenarios that could be used to test BCPs.

Updated tooltip for 26/27*:* *'It is recommended that BCPs and disaster recovery plans are regularly tested.*

Tabletop exercises or simulations could include a cyber-scenario (such as hacking), ***scenarios where the organisation has had a power cut and the phone line/internet goes down, staff working remotely and unable to access necessary systems, the office becomes unavailable for staff (for example through fire). These*** *should be used to test that the BCP is fit for purpose.* ***It is recommended that these are actioned annually and whenever the organisation has a significant change in suppliers, systems or processes.***

You should provide the date on which such a test was completed.'