Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit

IGDC • DHCW

Summary of Changes

Welsh IG Toolkit Question Set 2024/25 – General Medical Practices

Introduction

This document outlines the proposed changes to be made to the Welsh Information Governance Toolkit question set for submission in 2024/25.

There are no substantial changes this year and all proposed changes are a result of feedback received as part of the stakeholder question set consultation process. One question has been added to expectations exceeded following concerns raised by DHCW's Primary Care Services team regarding a high number of Mail Marshal breaches.

In summary:

- One additional question has been added to expectations exceeded.
- Thirteen questions have been reworded, there is no change to the requirements of these questions and previous answers and evidence will be carried over.
- Seven questions contained abbreviations that were not fully explained in the section. These have been amended to state the abbreviation in full in each section. All previous answers and evidence will carry over.
- Nine questions have had amendments to their corresponding tooltips, there have been no changes to these questions themselves.

Additional Questions

3 Information Security – Expectations Exceeded

Questions Reworded

1.2 Policies & Procedures

1.3 Training and Awareness

1.4 Individual Rights

1.5 ROPA and Lawful Basis

1.6 Contracts and Information Sharing

1.7 Risks & DPIAs

3 Information Security

Abbreviations Expanded

1.1 Leadership & Oversight

1.2 Policies & Procedures

1.3 Training & Awareness

1.7 Risks & DPIAs

2 Freedom of Information and Environmental Information Regulations

Tooltips Amended

1.3 Training and Awareness

1.4 Individual Rights

1.7 Risks and DPIA

1.8 Breach & Monitoring

4 Business Continuity

Additional Questions

3 Information Security – Expectations Exceeded

'Does the organisation take action to address Mail Marshal breach notifications received?'

Question added to expectations exceeded for 2024/25.

Questions Reworded

1.2 Policies & Procedures

'Does the organisation have up to date IG related policies and procedures in place for:

- Data Protection
- Records Management (including records retention)
- Information Security
- Data Quality '

Question reworded for 2024/25

'*Does the organisation have up to date IG related policies and procedures in place for:*

- *Data Protection/Information Governance*
- *Records Management (including records retention)*
- *Information Security*
- *Data Quality '*

'Does the organisation have policies or procedures in place that advise staff how to securely dispose of confidential records that are no longer required?'

Question reworded for 2024/25

'Does the organisation have policies or procedures in place that advise staff how to securely dispose of confidential records/data that is no longer required?'

1.3 Training and Awareness

'The IG and data protection TNA meets the needs of all staff and includes key areas of IG and data protection including:

- handling requests for information
- sharing of staff and patient personal information
- information security
- breaches of personal information
- records management'

Question reworded for 2024/25

'Does the IG and data protection TNA meet the needs of all staff and includes key areas of IG and data protection including:

- *handling requests for information*
- *sharing of staff and patient personal information*
- *information security*
- *breaches of personal information*
- *records management'*

1.4 Individual Rights

'Does the organisation have processes for dealing with requests to exercise the range of individual rights under data protection legislation including:

- Right to be Informed
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability
- Right to Object
- Rights relating to automated decision making'

Question reworded for 2024/25

'Does the organisation have a procedure in place for dealing with requests to exercise the range of individual rights under data protection legislation including:

- *Right to be Informed*
- *Right of Access*
- *Right to Rectification*
- *Right to Erasure*
- *Right to Restrict Processing*
- *Right to Data Portability*
- *Right to Object*
- *Rights relating to automated decision making'*

'Do all staff know how to recognise a request from an individual under data protection legislation, and their responsibilities to ensure any such request is dealt with?'

Question reworded for 2024/25

'Does the organisation take steps to make all staff aware of how to recognise a request from an individual under data protection legislation, and their responsibilities to ensure any such request is dealt with?".

'Do staff know how to inform individuals where to locate privacy information and how they can exercise their rights?'

Question reworded for 2024/25

'Does the organisation take steps to make all staff aware of how to inform individuals where to locate privacy information and how they can exercise their rights?'

'Privacy information includes:

- the identity and contact details of the controller
- the contact details of the data protection officer
- the purposes of the processing and the lawful basis being relied upon
- the organisations who personal information is shared with
- the period for which personal data will be retained
- the existence of individual rights
- the right to lodge a complaint with the ICO'

Question reworded for 2024/25

'Does privacy information include:

- *the identity and contact details of the controller*
- *the contact details of the data protection officer*
- *the purposes of the processing and the lawful basis being relied upon*
- *the organisations who personal information is shared with*
- *the period for which personal data will be retained*
- *the existence of individual rights*
- *the right to lodge a complaint with the ICO'*

1.5 ROPA and Lawful Basis

'The organisation has a formal 'Record of Processing Activities' (ROPA) that:

- is regularly reviewed to ensure that it remains accurate and up to date
- documents the lawful basis, or bases, relied upon for different processing activities
- documents the purpose for the processing of personal information for each activity on the ROPA'

Question reworded for 2024/25

'Does the organisation have a formal 'Record of Processing Activities' (ROPA) that:

- *is regularly reviewed to ensure that it remains accurate and up to date*
- *documents the lawful basis, or bases, relied upon for different processing activities*
- *documents the purpose for the processing of personal information for each activity on the ROPA'*

1.6 Contracts and Information Sharing

'Does the organisation ensure all contracts for suppliers, contractors, data processors and third parties are documented in a log or register?'

Question reworded for 2024/25

'Does the organisation ensure all contracts for suppliers, contractors, data processors and third parties are documented in a log, register or registers as appropriate?'

'The organisation ensures that security and confidentiality clauses/agreements are in place for:

- Permanent staff
- Temporary and agency staff
- Students and volunteers
- Locum workers'

Question reworded for 2024/25

'Does the organisation ensure that security and confidentiality clauses/agreements are in place for:

- *Permanent staff*
- *Temporary and agency staff*
- *Students and volunteers*
- *Locum workers'*

1.7 Risks & DPIAs

'Are staff aware of the need to consider a DPIA and the process to be followed?'

Question reworded for 2024/25

"Does the organisation take steps to make all staff aware of the need to consider a Data Protection Impact Assessment (DPIA) and the process to be followed?"

3 Information Security

'Staff access to systems is:

- monitored and audited
- and staff are informed that access to IT systems is monitored and audited'

Question reworded for 2024/25

'Is staff access to systems:

- *monitored and audited*
- *and staff are informed that access to IT systems is monitored and audited'*

'Routine information security checks/audits are regularly conducted that consider compliance with information security policies and procedures and:

- Any identified areas of concern are included in an information security improvement plan and escalated appropriately
- Information security audits outcomes are reported to the senior management team or Board'

Question reworded for 2024/25

'Are routine information security checks/audits regularly conducted that consider compliance with information security policies and procedures and:

- *Any identified areas of concern are included in an information security improvement plan and escalated appropriately*
- *Information security audits outcomes are reported to the senior management team or Board'*

Abbreviations Expanded

1.1 Leadership & Oversight

'Have one or more individuals been assigned responsibility for information governance (IG) and data protection?'

1.2 Policies & Procedures

'Does the organisation have policies or procedures in place to assess any data breaches and if required, report them to the Information Commissioner's Office (ICO) within the statutory time frames?'

'Does the organisation have effective and up to date Freedom of Information (FOI) & Environmental Information Regulations (EIR) procedures and relevant guidance outlining high level responsibilities?'

1.3 Training & Awareness

'Have all staff with operational responsibility for IG and data protection received appropriate training to carry out their role, including refresher training or relevant continued professional development (CPD) activities?'

1.7 Risks & DPIAs

'When carrying out a DPIA, are staff aware they need to seek the advice and guidance of the Data Protection Officer?'

'Where the DPIA identifies any residual high risks, is there a process for the Information Commissioner's Office (ICO) to be consulted, prior to processing commencing?'

2 Freedom of Information and Environmental Information Regulations

'Has the Information Commissioner's Office (ICO) Model publication scheme or an organisational ICO approved scheme been adopted and made available to members of the public via the organisation's webpage?'

Tooltips Amended

1.3 Training and Awareness

'Does the TNA include induction and refresher training for all staff, regardless of how long they will be working for the organisation, their grade or contractual status?'

Supporting information tooltip expanded for 2024/25

'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 within one month of their start date.'

'Are all staff required to complete mandatory IG refresher training at appropriate intervals?'

Supporting information tooltip expanded for 2024/25

'All staff within NHS Wales are required to undertake IG mandatory training on commencement of employment (within one month of their start date) and every two years.

All staff includes:

- Staff members

- GPs and GP Partners

- Directors/ Trustees

- Locums

- Agency workers

- Students

- Trainees

- Secondees

- Volunteers

- Contracted third parties'

1.4 Individual Rights

'Does the organisation have a procedure in place for dealing with requests to exercise the range of individual rights under data protection legislation including:

- Right to be Informed
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability
- Right to Object
- Rights relating to automated decision making'

Supporting information tooltip expanded for 2024/25

'UK GDPR provides the following rights for individuals:

- *The right to be informed*
- *The right of access*
- *The right to rectification*
- *The right to erasure*
- *The right to restrict processing*
- *The right to data portability*
- *The right to object*
- *Rights in relation to automated decision making and profiling*

Organisations must have a policy and procedures in place documenting how an individual can exercise their rights. This may be captured in a single policy/procedure, or it may be separated out, for example you may have a separate subject access request procedure. Your

procedures should account for the different types of personal data you process including, but not limited to, health records, staff records, emails and other communication methods and CCTV.

Instructions for individuals of how to make a request must be made available to them, such as through privacy notices.'

'Does the organisation take steps to make all staff aware of how to recognise a request from an individual under data protection legislation, and their responsibilities to ensure any such request is dealt with?'

Supporting information tooltip expanded for 2024/25

'All staff should receive training or guidance on what constitutes an individual rights request and the next steps required. Staff should be able to recognise a request, whether written or verbal, know who the request needs to be forwarded to for processing and understands the importance of doing so promptly due to the legislative time frames that apply. Staff should have an understanding that individual rights apply to all personal data processed by the organisation including, but not limited to, health records, staff records, emails and other communication methods and CCTV.'

'Does privacy information include:

- the identity and contact details of the controller
- the contact details of the data protection officer
- the purposes of the processing and the lawful basis being relied upon
- the organisations who personal information is shared with
- the period for which personal data will be retained
- the existence of individual rights
- the right to lodge a complaint with the ICO'

Supporting information tooltip expanded for 2024/25

'Organisations are required to publish transparency information about their data processing activities which informs people about their rights under data protection legislation and how to exercise them. This is known as a privacy notice.

The Privacy notice should provide:

• your organisation's contact details

• the Data Protection Officer's contact details (if your organisation has one)

• if your organisation is not the Controller, the details of the Controller and their Data Protection Officer

• what personal data you are processing

• the purpose of your processing

• the names or categories of organisations the data will be shared with

• the lawful basis for processing

• a list of rights and how they apply to the processing you are undertaking

• the retention period for the data (in line with the Records Management Code of Practice for health and social care 2022)

• that individuals have a right to complain to the ICO

Where applicable to the processing, the following details should also be provided:

• what the legitimate interests are if this is your legal basis for processing

• details of data transfers to countries outside the UK and what safeguards are in place to protect the data

• where consent is used as a legal basis for processing how consent can be withdraw

• if there is a legal or contractual obligation to provide the organisation with personal data

• whether there is any automated decision making (including profiling) that has a legal or similar effect on data subjects. This must include meaningful information about the logic involved and potential effects.

Privacy information must account for all personal information you are processing, including that of patients, staff, and visitors (for example if their image is captured on CCTV).'

1.7 Risks and DPIA

'Does the process detail that a DPIA is considered:

- In advance of the processing of personal data commencing
- When contemplating changes to existing or new projects
- When contemplating existing or new services or systems'

Supporting information tooltip expanded for 2024/25

'A DPIA is only required in certain circumstances, such as where the processing is likely to result in a risk to the rights and freedoms of individual(s). However, it is good practice to undertake a DPIA when the process/project involves large-scale processing of sensitive personal information.

The organisation should consider the need for a DPIA when contemplating changes to existing or new projects, services and systems. This should be conducted in advance of the processing of personal data commencing. Where it is identified that there is likely to be a risk to the rights and freedoms of individual(s), a DPIA must be conducted. This includes,

monitoring publicly accessible places on a large scale, therefore, a DPIA must be completed for any surveillance systems in place, if this has not been completed prior to the implementation of the system, a DPIA should be completed in retrospect.

A DPIA is not a one-off exercise and should be seen as an ongoing process and be regularly reviewed.'

1.8 Breach & Monitoring

'Does the organisation have an incident management system in place to register, report and follow up on data breaches?'

Supporting information tooltip expanded for 2024/25

'Damage resulting from potential and actual Information Governance, information security and Data Protection events should be minimised, and lessons learnt from them.

All incidents, suspected or observed, should be reported, recorded and investigated and appropriate actions taken to address the incident and learn lessons (where possible) so that they do not recur.

This includes weaknesses identified in systems design or operational procedures that potentially may result in an incident.

As a minimum you should document:

- the facts relating to the personal data breach,

- its effects, and

- any remedial action taken.

Organisations should have in place an appropriate incident recording system, that facilitates decision making about whether or not you need to notify the relevant supervisory authority and the affected individual.

This could be an incident management system like DATIX or a data base, paper-based recording system.'

4 Business Continuity

'Does the organisation have a business continuity plan that covers information and cyber security?'

Supporting information tooltip expanded for 2024/25

'Business Continuity Management (BCM) describes an organisation's attempt to predict, assess and counteract threats and risks that may cause or lead to significant disruption of all or part of the organisation's business functions. BCM examines the likelihood and impact of such disruptive events occurring, determines what the organisation can do to prevent or minimise the level of disruption and develop plans to affect a systematic and timely recovery.

Organisations should compile a collection of documented procedures and information in readiness for use in the event of an incident that interrupts normal business function to ensure critical business activity is maintained at an acceptable level.

Specifically, these plans should cover events of IT System failure in the event of information security or cyber security events.

All continuity plans should have privacy-by-design baked in, as the backup process could introduce other risks.

NHS England have a useful Business Continuity Toolkit which can be accessed here.'

'Has the business continuity plan been approved by the senior management team or Board?'

Supporting information tooltip amended for 2024/25.

The highest senior management level within the organisation has overall responsibility for data protection and information governance. The BCP should be approved by this forum, for example Practice Management Team, Senior Partners, or Board.