Cwm Taf Morgannwg University Health Board

Data protection audit report – Executive Summary

February 2022

ico.
Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

The purpose of the audit is to provide the Information Commissioner and Cwm Taf Morgannwg University Health Board (the Health Board) with an independent assurance of the extent to which the Health Board, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of the Health Board's processing of personal data. The scope may take into account any data protection issues or risks which are specific to the Health Board, identified from ICO intelligence or the Health Board's own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further

tailored the controls covered in each scope area to take into account the organisational structure of the Health Board, the nature and extent of the Health Board's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to the Health Board.

It was agreed that the audit would focus on the following areas

Scope area	Description
Governance and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UKGDPR and national data protection legislation are in place and in operation throughout the organisation.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore the Health Board agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from Monday 10 January to Wednesday 26 January 2022. The ICO would like to thank the Health Board for its flexibility and commitment to the audit during difficult and challenging circumstances.

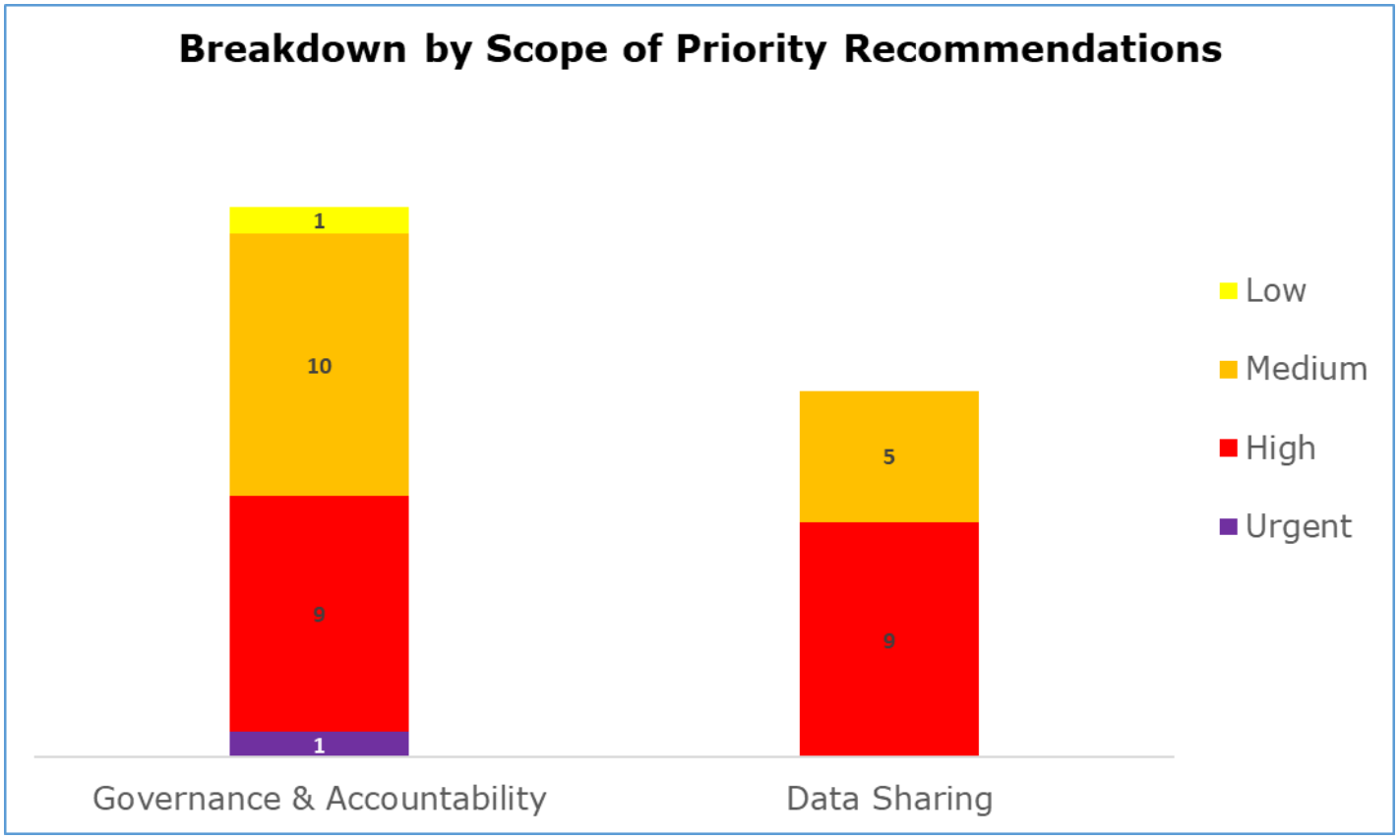
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Health Board in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. The Health Board's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance and Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Data Sharing	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

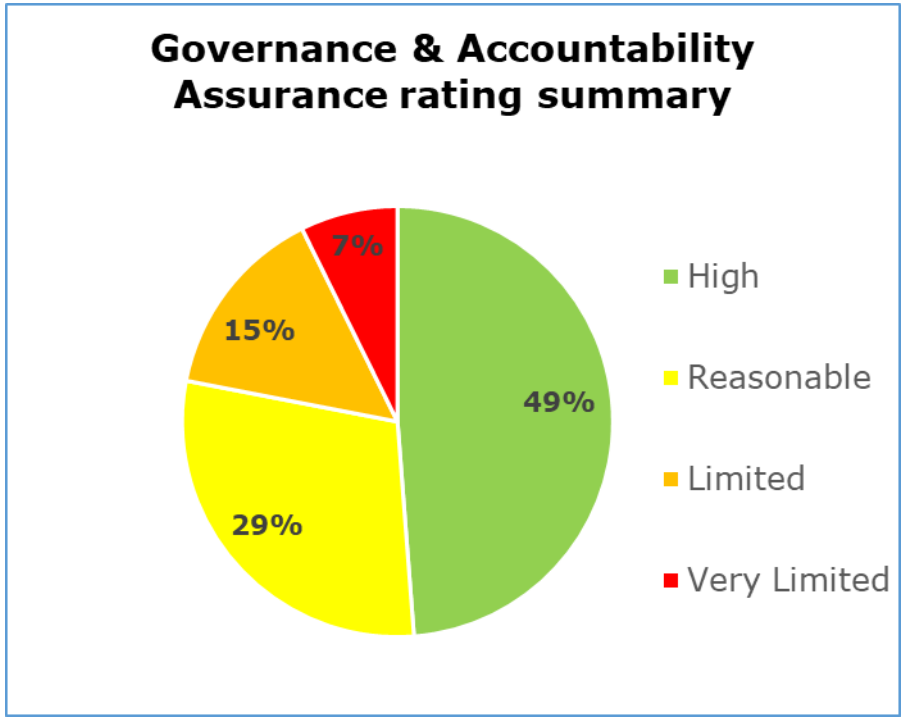
Priority Recommendations



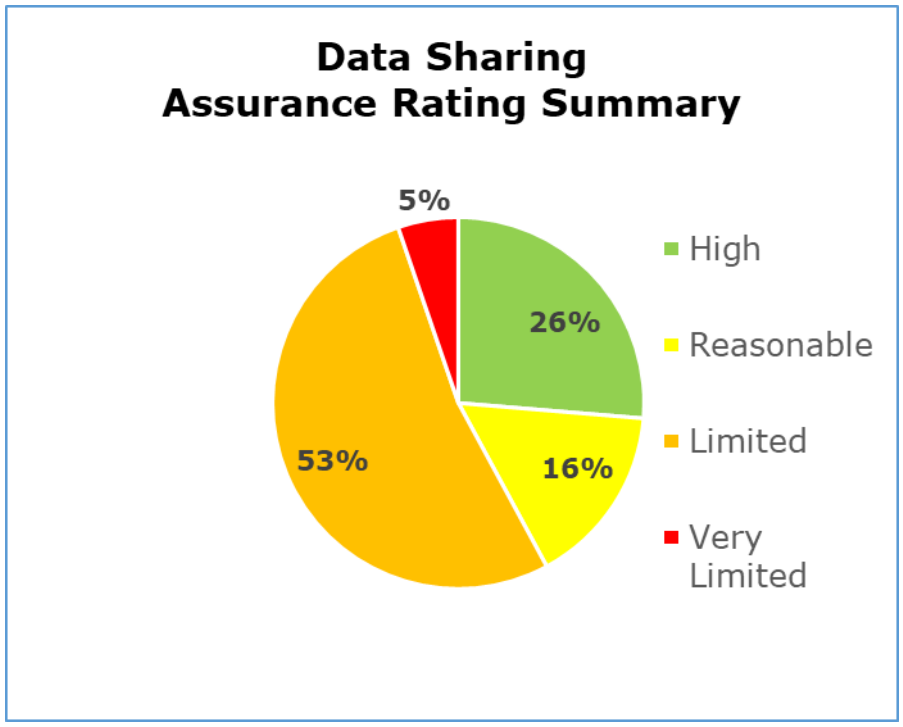
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 1 urgent, 9 high, 10 medium and 1 low priority recommendations
- Data Sharing has 9 high and 5 medium priority recommendations

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 49% high assurance, 29% reasonable assurance, 15% limited assurance, 7% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. 26% high assurance, 16% reasonable assurance, 53% limited assurance, 5% very limited assurance.

Areas for Improvement

Governance and Accountability:

- There is no Appropriate Policy Document (APD) in place to document the Health Board's justification for processing special category or criminal offence data, in accordance with current data protection legislation.

- The Health Board should consider whether the Data Protection Officer (DPO) is able to effectively fulfil the role of DPO as they are also Head of Information Governance, running a small and very busy information governance team. The DPO function requires further strengthening with the provision of a written description as to how the DPO role achieves operational independence and a reporting pathway to senior management. The Senior Information Risk Officer (SIRO) not being a Board member is also a risk to the strength of the information governance oversight within the Health Board.

- Training compliance and specialist training provision in data protection requires improvement. There is a need to raise the compliance rate for mandatory information governance training and ensure that appropriate additional training is given to all staff with specialised roles in data protection.

- There is no overall Record of Processing Activities (ROPA) based on a comprehensive data mapping exercise to give the Health Board assurance that it has full knowledge of all its processing of personal data.

Data Sharing:

- There is a lack of assurance that there are appropriate information sharing agreements, signed by senior management of all relevant parties, for all routine data sharing activities between the Health Board and third parties.

- Inconsistent methods across the Health Board for maintaining records of responses, approval and quality assurance for individual third party requests means that there is a risk of inadequate oversight as to how these requests are being handled.

- There is no process or schedule to review information sharing agreements on a regular basis to ensure that the activities continue to be lawful.

Best Practice

The Health Board's Data Protection Impact Assessment (DPIA) template includes a section asking whether automated decision making is involved, prompting consideration as to the legal or other significant effects on individuals.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Cwm Taf Morgannwg University Health Board.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Cwm Taf Morgannwg University Health Board. The scope areas and controls covered by the audit have been tailored to Cwm Taf Morgannwg University Health Board and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.