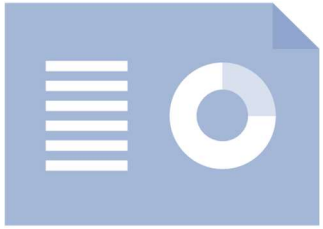
Cwm Taf Morgannwg University Health Board

Data protection audit report

February 2022

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

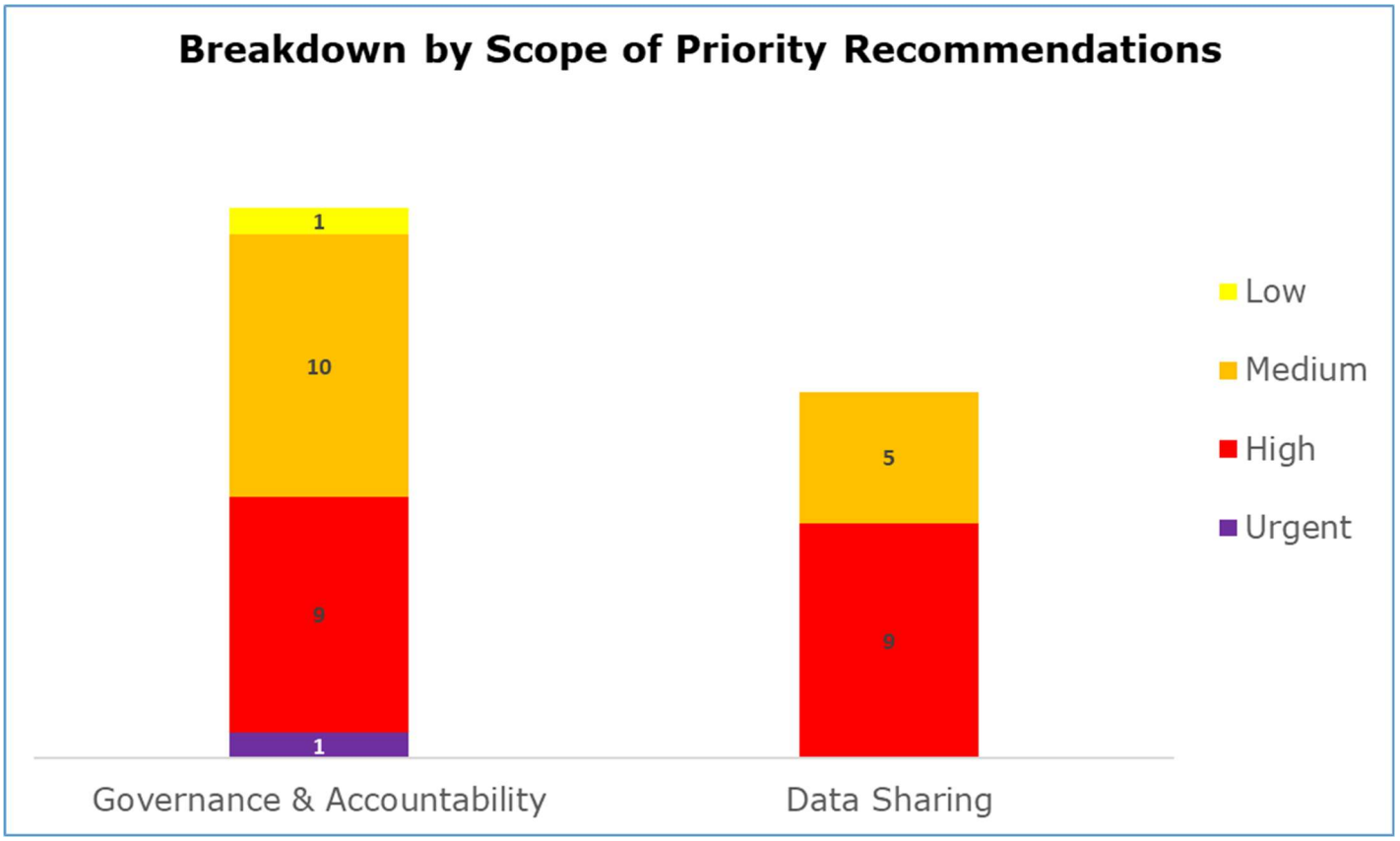
implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. The Health Board's priorities and risk appetite may vary and, therefore, they should undertake 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.

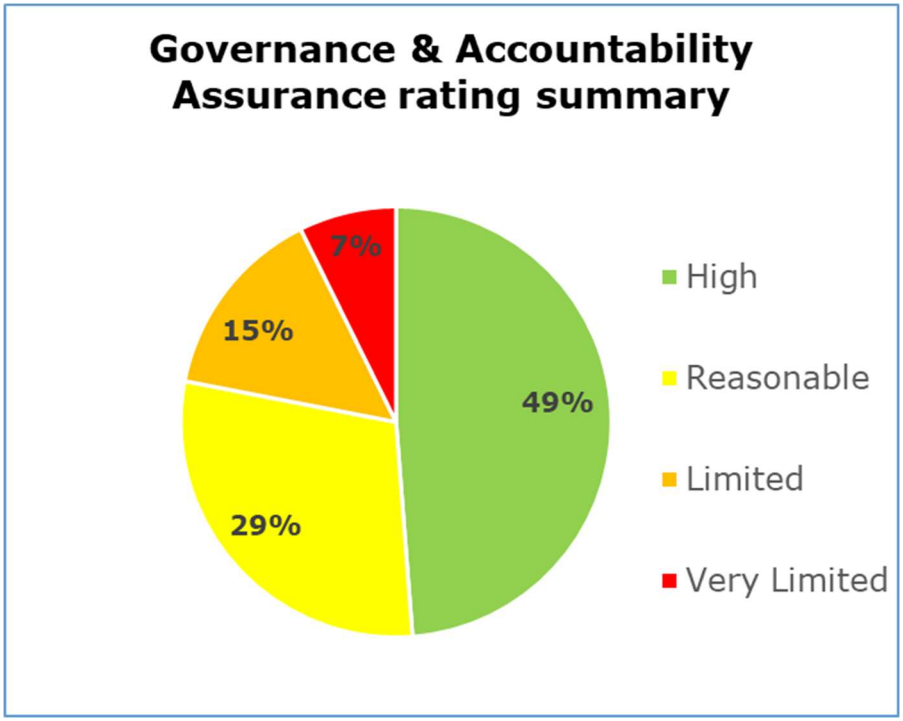
Priority Recommendations



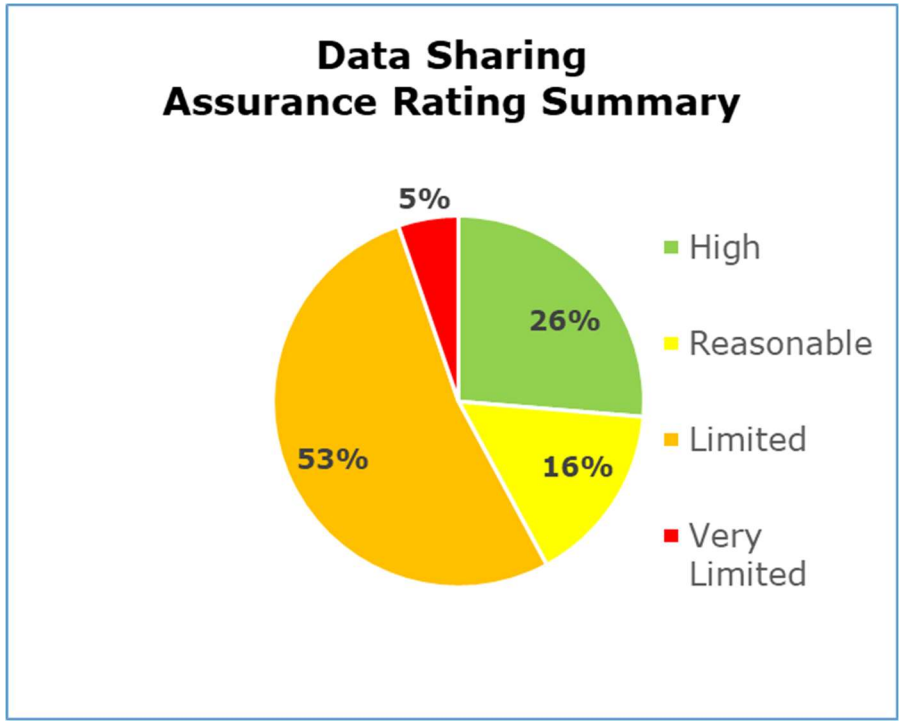
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- 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.

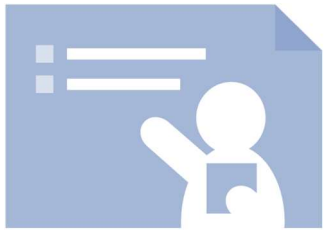
- Inconsistent methods across the Health Board for maintaining records of responses, approval and quality assurance for individual third party requests means that there is a risk of inadequate oversight as to how these requests are being handled.

- 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.

Audit findings



The tables below identify areas for improvement that were identified in the course of our audit; they include recommendations in relation to how those improvements might be achieved.

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is a management framework, including a delegated process of accountability and responsibility from the Board down, to support the information governance management agendas.	A01. The role of the Senior Information Risk Officer (SIRO) does not currently sit with a post which is at Board level within the Health Board. There may be a risk of inadequate accountability regarding risks if the ultimate risk owner is not at Board level.	A01. The Health Board should consider returning the role of SIRO to a post which sits on the Board to ensure information risk oversight at the highest level.	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is a Data Protection Officer in place with designated responsibility for data protection compliance.	A02 a. The Data Protection Officer (DPO) is also Head of Information Governance for the Health Board. Information governance is a small team within the Health Board, and there is a risk that the time which the Head of Information Governance is obliged to give to that role means that they do not have sufficient time resource to fulfil the role of DPO. A02 b. Although the Job Description for the Head of Information Governance states that the post holder will act as DPO for the Health Board, there is no description of the responsibilities of the DPO.	A02 a. The Board should consider whether the information governance function within the Health Board is adequately resourced in order to ensure that the DPO has the time to carry out their function. A02 b. To ensure that role of the DPO is understood and documented within the Health Board, there should be a clear description of the requirements and responsibilities of the role as outlined in the UK GDPR.	High
The DPO role has operational independence and appropriate reporting mechanisms are in place to senior management	A03. There is no written explanation as to how the DPO will have operational independence and an appropriate reporting pathway to senior management. This could lead to non conformance with UKGDPR Articles 37, 38, and 39.	A03. To ensure that role of the DPO is understood and documented within the Health Board, there should be a clear description of how the DPO will have operational independence and appropriate reporting mechanisms to senior management.	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
Operational roles and responsibilities have been assigned to support the day to day management of all aspects of information governance	A04. Information provided to auditors shows some discrepancies and errors in relation to operational roles and responsibilities for data protection, as follows: The Records Management Policy states that the Medical Records Manager is responsible for Health Records, while the Records Management Procedure states the Head of Digital Records is responsible for the overall management of the Health Records service within the Health Board. The 'General Requirements' section of various job descriptions is out of date as it refers to the Data Protection Act 1998. The Subject Access Request (SAR) procedure states that various directorates process requests centrally in teams, but staff in the integrated Locality Groups indicated that they also provide responses to subject access requests, in addition to providing complainants with medical records in relation to their complaints.	A04. The Health Board should ensure that responsibilities for the day to day management of information governance are clearly and accurately stated in documentation and reflected in practice to ensure that these responsibilities are carried out effectively and without breach of legislation.	Medium
There are local level operational meetings where data protection, records management and information security matters are discussed.	A05. Data protection issues are not covered in depth in meetings at Integrated Locality Group level This may lead to the risk of direction from senior management not being implemented or embedded on a local level, and operational level issues not being communicated or reported to senior management in a timely fashion.	A05. The Health Board should ensure that local level operational meetings include data protection, information security and records management as standard discussion points, to improve communication in both directions between operational and senior management levels.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
Where the organisation is required by Schedule 1 or Part 3 section 42 of the DPA18 to have an Appropriate Policy Document (APD) in place, the document in place is sufficient to fulfil the requirement.	A06. The Health Board does not have an Appropriate Policy Document (APD) in place in order to ensure that it has properly considered and documented its justification for processing personal data as required by Schedule 1, and / or section 42 of the DPA18. See also Data Sharing non-conformity B04	A06. The Health Board should consider whether it is required to have an APD in place, and if so, should ensure that one is drawn up to meet the requirements of the legislation to appropriately document its justification for processing personal data. See also Data Sharing non-conformity B04	Urgent
Policies and procedures are approved by senior management and subject to routine review to ensure they remain fit-for-purpose.	A07. Some policies and procedures shown to auditors were past the date due for review, namely: The Incident Reporting Policy was due for review in June 2016 and the Personal Data Breach management procedure was due for review March. The document 'Contract Requirements and Planning' refers to the Data Protection Act 1998. Documents containing outdated information or giving incorrect directions could lead to staff breaching data protection regulations.	A07. The Health Board should ensure that all policies and procedures are reviewed in line with their review date so that staff have access to correct information in order to avoid data protection breaches.	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
Refresher training is in place and delivered in a timely manner to all staff including temporary and agency staff etc.	A08. KPI figures show that the compliance rate for staff completing their mandatory Information Governance training is below 75%. This leads to a risk of staff breaching data protection legislation by forgetting their training, or being unaware of changes to procedure. There are additional difficulties in relation to Bank staff, and those who do not have daily access to computers for e-learning.	A08. The Health Board has a new team in Learning and Organisational Development who are putting in place new procedures to improve compliance with all mandatory training. The Health Board should ensure that these measures are implemented in a timely manner and monitor Information Governance training to ensure that the rate of compliance is raised, including among Bank staff and those who don't have regular access to e-learning.	High
There is provision of more specific DP training for specialised roles (such as the DPO, SIRO, IAOs) or particular functions e.g. records management teams, SAR teams, information security teams etc.	A09. Not all staff with specialised roles in data protection have received recent appropriate training. This gives a risk of breaches caused by lack of specialist knowledge. The Health Board may also not have a full picture of which staff are dealing with data protection concerns such as SARs (see non-conformity A04 above). See also Data Sharing non-conformity B02	A09. The Health Board should ensure that staff who require specialist information governance training are identified by means of a training needs analysis and given appropriate training to enable them to carry out their roles They should receive such training in a timely manner when restrictions due to the pandemic permit. See also Data Sharing recommendation B02	High
The organisation actively monitors or audits its own compliance with the requirements set out in its data protection policies and procedures.	A10. Restrictions due to the pandemic and resources in the information governance department have impacted on the ability of the Health Board to undertake visits to monitor compliance with data protection policies and procedures. This gives rise to a risk of non-compliance with data protection legislation not being corrected.	A10. The Health Board should look at means to monitor data protection requirements in its various localities and departments. This could be by information governance champions (see Observation A02 above), or through self-assessment checklists.	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There are data protection Key Performance Indicators (KPI) in place	A11. Key Performance Indicators (KPIs) relating to records management are not reported to the Information Governance Group (IGG). The IGG may therefore not have the oversight to assess where possible data protection breaches may occur.	A11. KPIs relating to records management should be reported to the IGG regularly to ensure that the group has full oversight of compliance with data protection requirements.	Medium
Performance to IG KPIs is reported and reviewed regularly.	A12. See above	A12. See above	Medium
There are written contracts in place with every processor acting on behalf of the organisation which set out the details of the processing	A13. Without undertaking a full data mapping exercise, the Health Board cannot be sure that all data processors acting on behalf of the Board have an adequate written contract in place. See also non-conformity A15 below.	A13. In order to ensure that all data processors are bound by an adequate contract, the Health Board should ensure that measure are taken to track and record all data flows.	High
The organisation takes accountability for ensuring all processors comply with the terms of the written contract(s)	A14. As not all contracts are subject to regular reviews, the Health Board may not have sufficient assurances as to whether processors continue to comply with terms and conditions, which could result in breaches of the legislation.	A14. The Health Board should ensure measure are in place to ensure that all data processors continue to abide by the terms of contracts.	Medium
The organisation has a process to ensure all processing activities are documented accurately and effectively	A15. The Health Board does not have a clear process for ensuring all processing activities are documented accurately and effectively. This means that further activities such as development of a Record of Processing Activities, Information Asset Registers, and risk assessments may be based on inaccurate or incomplete information.	A15. While it is understood that the pandemic will have an impact on the gathering of information regarding processing activities, the Health Board should ensure that measures are put in place to find out what personal data it holds. These should include information audits or data mapping exercises, as well as staff surveys and questionnaires.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is an internal record of all processing activities undertaken by the organisation	A16. The Health Board does not have an internal Record of Processing Activities (ROPA), so there is a risk that it does not have full knowledge of all processing activities and may be in breach of UKGDPR Article 30	A16. The Health Board should ensure that that there is in place a formal, documented, and comprehensive record of processing activities, which brings together the various documents where processing is already recorded, and which is based on a data mapping exercise.	High
The information documented within the internal record of all processing activities is in line with the requirements set out in Article 30 of the UKGDPR	A17. As there is no ROPA, the information documented by the Health Board in relation to its processing activities may not be in line with the requirements set out in UK GDPR Article 30	A17. The Health Board should ensure that its ROPA contains all information required by the legislation in relation to is data processing activities.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
The organisations privacy information or notice includes all the information as required under Articles 13 & 14 of the UKGDPR.	A18. Some of the fair processing information provided does not contain much detail as follows: The Privacy Notice on the Health Board's website does not give any information as to the type of data which is collected by the Health Board. The Privacy Notice on the Health Board's website does not provide any information about the retention periods used by the Health Board, and although the Your Information and your Rights leaflet is linked to, that in turn provides very little detail about retention periods. The Privacy Notice on the Health Board's website does not provide any detail about the rights of the data subject. While this is contained in the attached leaflets, site users may not see the links to the leaflets at the bottom of the page. See also Data Sharing non-conformity B03	A18. In order to ensure that the privacy Information is in line with the requirements of the legislation, the Health Board should provide all the elements required by data protection legislation. This includes the purposes of the data, the rights of the data subject and retention periods. To prevent privacy information from becoming too long, the initial page could provide brief headings with links to other and more detailed sections. See also Data Sharing recommendation B03	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
Privacy information is concise, transparent, intelligible and uses clear and plain language	A19 a. The Privacy information provided by the Health Board does not state whether it is available in other languages for those whose first language is not English or Welsh. A19 b. Privacy information provided by the Health Board is a combination of a privacy notice on the external website, and leaflets to which the website links for additional information. This means that data subjects have to look at several documents to find all information provided and may miss relevant information. As well as this, some of the information provided on the website privacy notice relates to information collected by the website itself rather than the collection of information for the day to day work of the Health Board.	A19 a. To ensure that all data subjects can understand the information presented to them, the Health Board should consider providing an option for privacy Information to be provided in languages other than English and Welsh. A19 b. The Health Board should revise the way privacy information is presented on its website to ensure that it is clear for users to follow and find the required information.	Medium
Existing policies, processes and procedures include references to DPIA requirements	A20. Relevant policies such the 'Contracts Requirements and Planning' and 'Reviewing Project Requests Information & Computer Technology (ICT) Process' do not contain references for the requirement for a DPIA.	A20. The Health Board should review policies relating to processes which may require a DPIA in order to ensure that the need for DPIAs have been built into the basic governance framework of the organisation.	Low

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
The organisation acts on the outputs of a DPIA to effectively mitigate or manage any risks identified.	A21. The DPIA procedure does not refer to a requirement to review the DPIA regularly or when the nature, scope, context or purposes of the processing changes, which means that any new risks may not be mitigated.	A21. The DPIA procedure should include reference to the requirement to review a DPIA regularly or when the nature, scope, context or purposes of the processing changes.	Medium

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
Information sharing decisions are documented and procedures are in place to ensure they are approved at the appropriate senior level.	B01 a. The Health Board has adopted the All Wales Information Governance Policy which identifies the Caldicott Guardian as the key individual for enabling appropriate information sharing. However, the policy does not cover the process to follow in the absence of the Caldicott Guardian if, for example, they were on annual leave. B01 b. The Health Board does not have a documented policy or procedure to follow should there be any need to share personal information in the event of an emergency or critical situation. If sharing decisions cannot be made and documented in a timely manner, there is a risk that the Health Board will be unable to share personal information or may share information inappropriately leading to non-compliance with Article 5(1) and 5(2) of the UK GDPR.	B01 a. The Health Board should document and implement the process and responsibility for making and approving data sharing decisions in the absence of the Caldicott Guardian should they be unavailable. The Health Board may wish to consider the appointment of a Deputy Caldicott Guardian for this purpose. This will help to ensure the Health Board can provide resilience in the absence of the Caldicott Guardian for approving the sharing of information. B01 b. The Health Board should implement an appropriate policy that covers the sharing of personal information in the event of an emergency or critical situation. The policy should include identifying who is responsible for approving and documenting any decisions around sharing information in these specific scenarios.	Medium

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
All staff likely to make decisions about sharing are adequately trained and made aware of their responsibilities.	B02. The Health Board has not identified all staff who may be involved in making decisions about data sharing. Additionally, the Health Board does not provide such staff with further training specifically around information sharing decision making beyond that which is included in the bi-annual mandatory IG training. Insufficiently trained staff are more likely to inappropriately share personal information or make unlawful decisions about the sharing of data, which may breach Articles 5(1) and 32 of the UK GDPR.	B02. The Health Board should ensure that all staff likely to make decisions about data sharing are identified, adequately trained and made aware of their responsibilities. Additional specialist data sharing training content including, where relevant, the heightened controls and the need for compelling reasons to share children's data, should be delivered at departmental induction and refreshed at an appropriate frequency, and should incorporate the requirements of the ICO's Data Sharing Code: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/ This will ensure that staff who may make a decision to share personal data are aware of the lawful requirements in doing so.	High

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
Individuals are informed about the sharing of their personal data.	B03. The privacy information that the Health Board provides to individuals about the sharing of their personal data does not meet the requirements of the UK GDPR. Specifically, the current patient privacy information available on the Health Board's website does not inform individuals about what personal data may be shared with other organisations or the lawful basis being relied on to share data. If individuals are not informed about the sharing of their personal information by the Health Board, this may lead to non-compliance with UK GDPR Articles 5(1)(a), 5(2), 12, 13 and 14.	B03. The Health Board should ensure that the privacy information it provides to individuals about the sharing of personal data meets the requirements of the UK GDPR.	High

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is a process to assess the legality of sharing and document any outcomes.	B04. The Health Board's process for assessing the legality of information sharing and the documenting of outcomes does not meet the requirements of the data protection legislation. The Health Board's Data Protection Impact Assessment (DPIA) procedure and template do not consider the Data Protection Act 2018 (DPA 2018) Schedule 1 conditions for processing of special categories of personal data and criminal convictions where necessary, nor the wider legal power to share information beyond the UK GDPR / DPA 2018. Without an adequate process to assess the legality of each sharing activity, the Health Board may not be able to sufficiently demonstrate why it believes the sharing to be legal which may breach UK GDPR Articles 5(1)(a) and (b), 5(2), 9 and 10.	B04. The Health Board should ensure that its process for assessing the legality of each information sharing activity and the documenting of any outcomes meets the requirements of the UK GDPR and DPA 2018.	Medium

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
Data sharing agreements have been agreed with all parties with whom personal data is routinely shared	B05. Not all staff that were interviewed during the audit have full confidence that every routine data sharing activity is covered by an appropriate sharing agreement. Additionally, a number of the Health Board's existing sharing agreements have not been signed by all parties to the specific agreement. This means that for some routine data sharing activities, certain sharing partners may not be committed to complying with any specific terms or requirements, which will increase the risk of inappropriate and unlawful information sharing between the Health Board and other parties. This may result in a personal data breach and non-compliance with the ICO's Data Sharing Code and the UK GDPR Articles 5(1), 5(2) and 32.	B05. The Health Board should ensure that all of its routine data sharing activities are covered by an appropriate agreement that has been signed by the senior management of all relevant parties, and that each agreement is made available to the staff involved in the actual sharing.	High

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
Data sharing agreements are sufficiently detailed, and provide sufficient direction to both parties to ensure that the requirements of the legislation are met	B06. The sharing agreements to which the Health Board is a party are not sufficiently detailed in all cases to meet the requirements of the data protection legislation and the ICO's Data Sharing Code. Not all sharing agreements state the DPA 2018 Schedule 1 conditions for processing of special categories of personal data and criminal convictions where necessary, nor the wider legal power to share information beyond the UK GDPR / DPA 2018. It was also identified that sharing agreements do not cover partners' responsibilities and procedures for responding to Freedom of Information (FOI) requests and the need to include certain types of information in FOI publication schemes. Where routine, and therefore high volume, data sharing takes place without a sufficiently detailed sharing agreement, there is an increased risk of inappropriate and unlawful sharing.	B06. The Health Board should ensure its sharing agreements are sufficiently detailed and meet the requirements of the data protection legislation and the ICO's Data Sharing Code: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-agreements/#include	Medium

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
Data sharing agreements are reviewed on a regular basis	B07 a. The Health Board does not schedule regular reviews of its sharing agreements (both ISPs and DDAs), nor where there has been a change in circumstances in the rationale for the data sharing or following a significant complaint or security breach. There is a risk that older sharing agreements which may not have been subject to regular reviews become unfit for purpose over time, which increases the likelihood of unlawful sharing. B07 b. The discussion of sharing agreements is not a standing agenda item at the Information Governance Group (IGG) or Digital and Data Committee (DADC) meetings, which means that the Health Board may not have sufficient senior oversight of any relevant changes or newly identified risks within the organisation's portfolio of sharing agreements. This means that there may be an increased risk of unlawful sharing which could result in a personal data breach and non-compliance with the UK GDPR and the ICO's Data Sharing Code.	B07 a. The Health Board should ensure that it implements a process to review its sharing agreements on a regular and ongoing basis to provide assurance that each agreement is working as expected with relevant partners, and the specific sharing activity continues to be lawful. B07 b. The Health Board should ensure that it has regular and sufficient senior oversight of its data sharing arrangements including higher risk agreements that could be subject to a change in circumstances in the rationale for data sharing, or those that have received a significant complaint or security breach.	High

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is a log or record of all data sharing agreements	B08. The Health Board does not have a single centralised log for all its information sharing agreements. This may make it more difficult for those staff involved in sharing personal data to determine whether a specific sharing activity is covered by an existing valid agreement. As a result, there is an increased likelihood of routine data sharing taking place outside of a valid agreement, or the potential for a duplicate agreement to be created for the same sharing activity.	B08. The Health Board should ensure that it has a single centralised log to record details of its information sharing agreements, including the nature of each sharing activity and the partners to the specific agreement, and that this log is accurate, up to date and complete. Additionally, the Health Board should implement measures for the log to be reviewed at appropriate intervals so that any changes, including updates to reflect any new, lapsed or expired agreements, can be actioned in a timely manner.	Medium

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
There are controls in place to ensure that the data shared is not retained for longer than necessary by all parties, including any data processors.	B09. Specific retention periods and disposal arrangements for shared personal data are not included in all information sharing agreements and data processor contracts. Additionally, the Health Board does not have adequate processes or controls in place to check that any stated retention periods and disposal arrangements are being adhered to by its sharing partners and processors. There is an increased likelihood of a personal data breach where shared personal data is being retained by sharing partners and processors for longer than has been agreed, or is not being disposed of in line with specified arrangements.	B09. The Health Board should ensure that all existing and new information sharing agreements and data processor contracts contain specific retention periods and disposal arrangements for any personal data shared between parties. The organisation should also ensure that there is an appropriate mechanism in place to provide assurance that shared data has been deleted, destroyed or returned once the purpose for sharing data is completed or relevant retention periods have been reached.	High

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
There are appropriate levels of access control in place on all systems which process shared data	B10. The Health Board does not routinely obtain documented access control policies and evidence of formal implementation of those policies by its sharing partners. Additionally, the Health Board does not regularly review access control measures over the organisation's systems that are accessed by its sharing partners. If effective and up to date access controls with sharing partners are not in place, there is a risk that personal data may be accessed inappropriately which may breach UK GDPR Articles 5(1)(f), 5(2) and 32.	B10. The Health Board should ensure that it has robust and effective access control review and monitoring measures in place to provide assurance that only nominated points of contact within its sharing partners can access shared data. This includes personal data that is shared by giving partners' staff access to the Health Board's systems.	High

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
There are effective incident management procedures in place with all sharing partners	B11. The Health Board does not routinely seek documented incident management procedures from its sharing partners or assurances that formal incident management procedures have been implemented by them. Additionally, the sharing agreements to which the Health Board is a party do not contain defined incident reporting deadlines in every case. If effective incident management procedures are not in place and documented in sharing agreements, there is an increased risk that the outcome of an incident may be worse for individuals affected and breaches may not be reported to the ICO within the required 72 hours. This may result in a breach of UK GDPR Articles 5(1)(f), 5(2), 32, 33 and 34.	B11. The Health Board should satisfy itself that its sharing partners have implemented effective incident management procedures so that actual or near miss security incidents involving shared data are immediately reported to the Health Board. This will enable the organisation to assess the likely risks to individuals' rights and freedoms that result from the breach, and allow the statutory reporting of certain breaches to the ICO within the required 72 hours.	High

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
Procedures are in place for responding to ad Hoc 3rd party requests for personal data	B12. The Health Board does not have a single documented procedure for responding to ad hoc third party requests for personal data that covers all teams that handle such requests. Currently, different departments have their own localised procedures, which are not sufficiently detailed or regularly reviewed in all cases, meaning that ad hoc third party requests are not being handled in a consistent manner. As a result, the Health Board may not have sufficient oversight of how the organisation handles these requests and the lack of consistency may increase the risk that personal information may be disclosed inappropriately.	B12. The Health Board should ensure that all teams that handle ad hoc third party requests for information are doing so in a consistent manner, and that any documented procedures are sufficiently detailed, reviewed at appropriate intervals and communicated to all relevant staff.	High

Data Sharing			
Control	**Non-conformity**	**Recommendation**	**Priority**
Records are kept of responses, approval, and quality assurance against legislative requirements for 3rd party requests for personal data	B13. The Medical Records department stores documentation relating to each ad hoc third party request, including a copy of any response, as a hard copy in lever arch files stored on shelves. The team at the Royal Glamorgan Hospital also records ad hoc police requests for personal data in a handwritten book held in the office. There is a lack of consistency in how relevant departments within the Health Board maintain records of responses, approval and quality assurance against legislative requirements for ad hoc third party disclosures, and a risk that the organisation does not have sufficient oversight of how individual disclosure requests are being handled. This may make it more difficult for the Health Board to meet its obligations under UK GPDR Article 5(2).	B13. The Health Board should ensure there are consistent and appropriate mechanisms in place for tracking and monitoring ad hoc third party disclosure requests, including keeping records of responses, approval and quality assurance against legislative requirements. Such mechanisms should also provide sufficient oversight to enable the Health Board to regularly assess the quality of how disclosure requests are being handled across all relevant departments for audit, monitoring and investigative purposes.	High
There are active operational controls and processes in place to ensure that data shared in bulk is in accordance with data protection legislation.	B14. There is no documented process or procedure in place that covers bulk transfers of personal data. Without a documented process or procedure, bulk transfers of personal data may be done without sufficient scrutiny or approval, leading to an increased risk of a personal data breach or incomplete/inaccurate personal data being shared.	B14. The Health Board should ensure that there is a sufficiently detailed policy or procedure in place to cover bulk transfers of personal data so that all staff involved in such transfers are aware of the authorisation processes required prior to releasing any data or making adjustments to existing data sets.	Medium

Observations

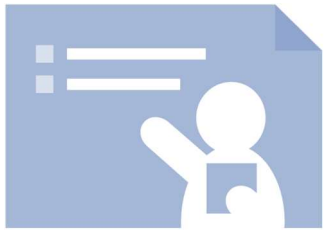
The tables below list observations made by auditors during the course of the audit along with suggestions to assist the Health Board with possible changes.

Governance & Accountability	
Control	**Observation**
There is an Information Management Steering Group, Committee, or equivalent, in place, which is responsible for providing the general oversight for information governance and data protection compliance activity within the organisation.	A01. The Digital and Data Committee into which the Information Governance Group Reports has had some meetings suspended due to the pandemic. The Health Board should ensure that these meetings are reinstated when practicable.
There are local level operational meetings where data protection, records management and information security matters are discussed.	A02. To support information governance in the ILGs, the Health Board may wish to consider having information governance champions who could act as a point of contact between the ILGs and the central information governance team, and provide responses to simple enquiries which would help take some work from the central team.

Governance & Accountability	
Control	**Observation**
Policies and procedures are readily available to staff and are communicated through various channels to maintain staff awareness	A03. In order to ensure that as many staff as possible have read policies and guidance, the Health Board should consider extending the use of 'MetaCompliance' Policy Management Software, and continue to look at means of seeing if messages have been read as part of the digital transformation programme.
The lawful basis and condition(s) for processing personal data, special category data and data relating to criminal convictions and offences has been identified appropriately, defined and documented internally.	A04. While the Information Asset Register and individual DPIAs identify the legal bases and conditions for processing personal data, once the Health Board has an Appropriate Policy Document and ROPA in place, the lawful bases and conditions by which the Health Board process data will be documented in a manner easy to access and update.
Individuals are provided with privacy information at the time their personal data is collected from them or obtained.	A05. The production of printed information such as privacy notices has stopped as an infection control measure in the pandemic. The Health Board is advised however to look into producing privacy notices in a printed form as soon as this is deemed possible, so that data subjects who may not be regular internet users are provided with fair processing information.

Data Sharing	
Control	**Observation**
Records are kept of responses, approval, and quality assurance against legislative requirements for 3rd party requests for personal data.	B01. The Health Board may also wish to review and satisfy itself that storage arrangements for all manual documentation relating to individual ad hoc third party requests provide an adequate level of security to reflect the level and sensitivity of the personal data being processed for this purpose.

Appendices



Appendix One – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations - These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations - These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations – These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Appendix Two:

Cwm Taf Morgannwg University Health Board
Audit survey results

Survey closed on 25/01/2022 with **93** responses

---

1. Do you know who Cwm Taf Morgannwg University Health Board's Data Protection Officer (DPO) is?

Yes	39
No	52
Does not have a DPO	0

---

2. Since joining the Health Board, which of the following policies have you been asked to confirm that you have read and understood?

All Wales Information Governance Policy	68
Information Security Policy	62
Record Management Policy	47
None of the above	13

---

3. Which methods are used to communicate new and updated policies to you?

Intranet	77

Staff meetings	31
Electronic bulletins / briefings	49
These are communicated to me in other ways	13
These are not communicated to me	6

---

4. Are policies and procedures available to read on Cwm Taf Morgannwg University Health Board's intranet site?

Yes	81
No	0
Don't know	10

---

5. When did you last undertake training on data protection / information security?

Less than 6 months ago	26
6 - 12 months ago	24
12 - 24 months ago	21
More than 24 months ago	15
Never	4

---

6. Do you have sufficient time to complete mandatory training?

Yes	65

No	25

---

7. Do you have sufficient access to equipment to undertake mandatory training?

Yes	86
No	5

---

8. Does your line manager or another person in your department encourage you to complete your mandatory training in good time?

Yes	68
No	17
Don't know	5

---

9. What would happen if you did not complete training on time?

Reminder sent	62
Disciplinary action	0
Nothing	11
Don't know	17
Other	0

---

10. How are data protection, or information security issues or messages communicated to staff?

Team meetings	38
Intranet	71
Electronic bulletins/briefings	49
Other	13

---

11. Do you know who to contact for any data protection queries or advice?

Yes	58
No	33

---

12. Does your organisation provide any instruction on how to handle requests for personal data from third parties?

Yes	58
No	10
Don't know	22

---

13. Would you know what to do if you discovered personal data was inaccurate or not up to date?

Yes	66
No	10
Don't know	15

---

14. Would you know what to do if you discovered paperwork or equipment that held personal data was lost or stolen?

Yes	74
No	9
Don't know	8

---

15. Do you think you would be able to recognise a personal data breach?

Yes	74
No	4
Don't know	13

---

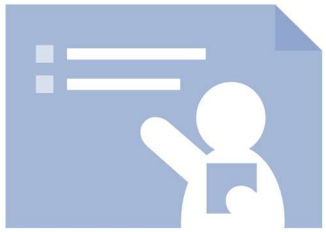
16. Are you familiar with the process of reporting a data breach if you became aware of one?

Yes	56
No	23
Don't know	11

17. How does Cwm Taf Morgannwg University Health Board inform individuals how their personal data is used, shared and secured?

Verbally	21
In leaflet form	21
On the internet	38
Don't know	44

Credits



ICO Audit Team

ICO Team Manager – Michael Thewlis
ICO Engagement Lead Auditor – Elizabeth McKay
ICO Lead Auditor – Ben Gnatiuk

Thanks

The ICO would like to thank Claire Northwell, Head of Information Governance and DPO, and Rebecca Walsh, Information Governance Officer for their help in the audit engagement.

Distribution List

This report is for the attention of Claire Northwell, Head of Information Governance and DPO, and Andrew Nelson, Chief Information Officer and SIRO.

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.