#REF!

ICO Data Protection Audit - Action Plan

Controller	Cwm Taf Morgannwg University Health Board
Report Date	Feb-22

Audit Action Plan							Audit Action Plan Update			
Ref	Control measure	Non-conformity	Recommendation	Priority	Accept / Partially Accept / Reject	Agreed Action	Update at 6 months (August)	ICO Officer's feedback - August 2022	December Update	February 2023 update
A01	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	Accept	The points raised by the auditors was considered. The SIRO assurance is discharged via the Digital and Data Committee, a sub committee of the main Board. We will review best practice for SIRO provision across NHS Wales	As a result of key personnel leaving the organisation the Director of Digital (Executive Level Position who attends Board Meetings) will take on the role of SIRO with effect from the 1st September 2022.		Complete	
A02	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	Accept	a)- Failure to deliver a robust and sustainable Information Governance Function is a risk on the Organisational Risk Register. The control measures and risk prioritisation exercise undertaken by the IG Team is captured and detailed in this risk assessment. Alternative ways of working have been explored with no sustainable solution identified. The fundamental risk treatment option to manage this risk, given the significant increase in activity in this area is an increase in resource. In this regard, an increase in resource has been included in the IMTP for 2022/2023 The issue of resource has been raised at an Executive Board level and continues to be considered. The training needs analysis (ref A10) will enable opportunities to identify IG Champions to support broader knowledge and resources for the function. A02 b) The Head of IG's JD has been amended to reflect the points raised and now clearly define the responsibilities and requirements.	A02.a) The Health Board has increased the risk on its Organisational Risk Register from a 16 to a 20 *(Datix Risk ID 4699 - Failure to deliver a robust and sustainable Information Governance Function)* to recognise that the fragility of the function has been further exacerbated by the departure of the Head of Information Governance at the end of July 2022 and the imminent Departure of the Information Governance Officer. This was reported to the Digital & Data Committee and Board. Recruitment to the Head of IG was unsuccessful and the Director of Digital having tested the market is reviewing the position further to commencing a further recruitment exercise. In alignment with the SIRO changes articulated in A01, the Chief Information Officer will hold the position of Data Protection Officer and will receive training within the next 2 months. A02.b) **COMPLETE -** The updated Job Description was used in the recent recruitment to the Head of Information Governance.	**A02.a** (high): Following recent and anticipated resignations by key IG team members, the Health Board should ensure that the issue over IG team resourcing is addressed as soon as possible and that any interim arrangements allow the Health Board to deliver a robust IG function in the near term.	Acting Head of IG in place, band 6 IG officer appointed and will commence in post around 1st Jan 23. JD not updated	Resource not improved. JD for CIO to include Data Protection Officer role not updated as Executive wish to proceed with further organisational change. Intention is for new post to take on Information, IG and Cyber and that they will fulfil DPO role.
A03	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	Accept	The Head of IG JD has been amended to reflect the clear operational independence and reporting pathway to Senior Management.	**COMPLETE** - The updated Job Description was used in the recent recruitment to the Head of Information Governance. Following the unsuccessful attempt to recruit to a Head of IG- the JD of the CIO will be amended to incorporate DPO and the wording adopted to reflect the clear operation independence and reporting pathway.	**A03** (medium): Before we can assess this recommendation as 'completed', we require confirmation that the JD for the CIO has been updated and approved to include a clear description of how their role as DPO will have operational independence and appropriate reporting mechanisms to senior management.	No progress	JD for CIO to include Data Protection Officer role not updated as Executive wish to proceed with further organisational change. Intention is for new post to take on Information, IG and Cyber and that they will fulfil DPO role.
A04	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	Accept	Board level responsibilities are clearly set out in Executive Portfolios. Job descriptions updated to clearly articulate leadership roles and responsibilities for; Director of Digital, SIRO, Caldicott Guardian and DPO. The Terms of Reference for the Health Board's Information Group is to develop and implement a framework for Information Governance across the organisation and to reinforce a strong ethos of Information Governance. The reports received at the meeting reflect the practice within the organisation. Job Descriptions for the Information Governance Team clearly state their IG responsibilities and the departmental reporting structure has recently been reviewed and captured in an organogram. Training provided on IG outlines individual responsibilities of all staff in relation to IG and also covers the roles of the IG team, and sources of advice and support. The DPO will raise the issue of references to the previous legislation with the recruitment team to ensure the clauses are updated. The Health Board has a suite of IG Policy Documents reflecting current procedures and practice. There is a dedicated SharePoint Page for Staff on IG Activity and sources for seeking advice.	A04.a) **COMPLETE** In addition to the update in column 'h' the following actions are also noted: Records Management Policy and Procedure have been amended to ensure consistency in relation to responsibilities. Reminders in relation to update the DPA Legislation has been shared with key roles within the Digital Directors portfolio. The latest recruitment to the Head of IG and IG Officer are up to date. The Job Matching Panel leads have also been asked to reflect the latest legislation in terms of any JD's that are received through them that sit outside the Director of Digital's remit. In terms of the SAR Procedure - the reference to directorates is another term for ILG's. There is no central SARS team these are managed and co-ordinated by service leads with advice from the central IG Team as required. The exception to this is corporate or workforce related SARs which are managed by the IG Team centrally. The managers of digital systems and the corporate warehouse have agreed and actioned a request to prioritise more of their time to their role as information asset owners. This has resulted in progress being made in refreshing the asset register and data flows and in ensuring that IG and cyber escalations are discussed in service meetings.	**A04** (medium): Whilst we are satisfied that the commentary provided is sufficient to meet the recommendation, the evidence presented will need to be updated to show that the IG function now comes under the Digital Directorate (evidence A04.1) and reflects any staff changes in the IG team (evidence A04.2).	No progress	
A05	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	Accept	The IG Team will link in with the meetings held with Workforce Business Partners and Learning & Development to raise IG awareness around compliance and risks. Links will be made with Operational Groups within ILGs and Central functions to discuss how they can embed as a standing agenda topic capturing IG risks and issues.	A05.a) The Health Board is currently implementing a new Operating Model and the governance arrangements in terms of the operational meeting structures that sit underneath the model are currently being mapped. This action has therefore been delayed until the new model is implemented and appropriate links within the new structure can be made.		Relationships within the wider informatics team have strengthened as has awareness of legal requirements. Increasingly this is ensuring that both IG and cyber matters are being discussed prior to implementation. Operational procedures have thus far prevented data sharing and applications being added to the network without the integrated DPIA, CSIA process being followed.	Relationships within the wider informatics team have strengthened as has awareness of legal requirements. Increasingly this is ensuring that both IG and cyber matters are being discussed prior to implementation. Operational procedures have thus far prevented data sharing and applications being added to the network without the integrated DPIA, CSIA process being followed.

A06	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	Accept	A Policy Document has been drafted and is on the agenda for the March 2022 meeting of the Information Governance Group. If endorsed, this will then be submitted to the Digital & Data Committee for approval.	A06.a) **COMPLETE** - the Information Governance Group approved the Appropriate Policy Document - (It was not required to be endorsed by the Digital & Data Committee). This has been published on the Information Governance SharePoint site.	**Completed**		
A07	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	Accept	The Health Board is currently undertaking a project to review approve its process for the management of Policies and Procedures which will support more timely review and monitoring of compliance through the Strategic Leadership Group. A policy schedule for IG related policy documents is received as a standing agenda item at the IG Group meetings.	A07.a) The Health Board is currently looking to secure additional resource through the review of the Operating Model to support the management of Policies within the Health Board. A short project was completed so that the overall position/ status of Health Board polices was clear. The Assistant Director of Governance and Risk has provided each Executive Lead with a Policy Status Schedule and is working with colleagues to support policy review prioritisation within the Health Board. This is a significant task and will be an ongoing action - work is underway but implementation will exceed July 2022. The IG Group receive the IG policy schedule as a standing agenda item for monitoring and assurance. All Wales Policies for NHS Wales Information Governance Policy , NHS Wales Information Security Policy, NHS Wales Internet Use Policy have currently been reviewed and out are out for comment with NHS Wales organisations with a deadline of the 26th August.		All Wales policies presently being reviewed, CTM are contributing to these.	All Wales policies presently being reviewed, CTM are contributing to these.
A08	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	Accept	An action plan for compliance improvement was endorsed by the People & Culture Committee in October 2021, since then L&D continue to support the organisation in improving compliance. Staff Induction. Compliance will feature more prominently in a new staff induction which will begin to be phased in from June 2022. Information Governance will be central to staff successfully completing their induction. New Starter E-Learning Training. Effective Jan 2022, all new starters are invited to attend training to equip them with the skills to complete their IG compliance training. All staff are required to complete IG compliance training within 30 days of commencing employment. Compliance Clinics. Effective December 2021, L&D now provide a range of clinics to all staff, these provide opportunity for staff to have 1:1 support in improving their IG compliance training. Reporting. Monthly reports are provided to HR staff and Line Managers on staff current compliance in IG. LM have an opportunity, via L&D, to attend additional training to run bespoke team reports to focus compliance activity in their own areas. HR Recover Plans. Heads of Workforce have dedicated recovery plans to address underperforming areas of compliance, allowing a more targeted approach to lower areas of compliance training. Communications. A dedicated area SharePoint area (effective Feb 2022) has been set up to provide staff with the key information required to complete compliance training. In addition L&D have published a Compliance Brochure to inform staff of compliance requirements, how to	A08.a) As at July 2022, Compliance for the information governance training continues to remain stable with no significant increase or decrease. The Health Board's current compliance with the Core Skills Training Framework is 72.19% which remains under the compliance rate of 85%. Virtual monthly training sessions continue to be offered. In addition to this, an email has been sent from the Head of IG targeting all staff that are currently showing as non-compliant on the ESR dashboard (in excess of 3000 staff). It is hoped that this will improve compliance. It should be noted that the delivery of training outside what is available through ESR will be significantly impacted by the departure of the Head of IG and IG Officer until these roles are successfully filled. An amendment to UHB procedures is under consideration which would require staff to have their IG training up to date in order for their active directory account (which provides access to the vast majority of the digital estate) to remain open. Some service continuity issues which will affect patient outcomes have been identified and options are being explored. Induction training in data protection for new clinicians has been arranged for the 8th September. Cyber awareness material has been produced in partnership with the police, with quarterly sessions due to run from September.	**In Progress - Not completed: A08** (high): Commentary indicates that additional measures have been introduced to improve refresher training compliance. However, the evidence provided suggests that these measures have not yet led to a noticeable improvement in compliance rates which continue to sit below the Health Board's target of 85%. Before agreeing that this has been completed, we would require evidence to show the impact of the new measures is leading to a noticeable and ongoing improvement in training compliance rates. This evidence can be provided at the December interim follow up, or if compliance rates are still low then at the final follow up in March 2023.	No progress	Compliance at 74%
A09	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	Accept	The HB will benchmark with other organisations to look to develop a training needs analysis that will support a greater understanding at a level of training within the organisation. This action will require close liaison with the L&D Dept. as to how this could be implemented In the meantime the HB will continue to offer monthly IG training and respond to individual requests for more specialist training as required	A09.a) Chief Information Officer and CSIO have attended the full week of NIST Cyber Security Professional (NCSP) training in June 2022 and there is an intention to complete further specialised training in the Autumn period for relevant people in cyber incident management, DPO, SIRO, IAO . All staff in the digital team have completed their mandatory IG training and are in the process of completing their cyber awareness training. Bespoke training for Subject Access training has now been rolled out to Claims / Concerns and mental health teams. Future sessions available as required. It should be noted that the delivery of training outside what is available through ESR will be significantly impacted by the departure of the Head of IG and IG Officer until these roles are successfully filled.	**A09** (high): We require evidence to show that a training needs analysis has been carried out to identify those staff that require specialist IG training, and that this training is being delivered to relevant individuals.	SIRO has attended refresher training in November 2022. No training needs analysis undertaken	No progress
A10	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	Partially accept	The HB will explore the introduction of IG champions, learning from others across NHS Wales where this model has been established. Recommendations will then be considered by the IGG Group. The HB undertakes the IG Toolkit assessment on an annual basis and this includes Health Records / Security / Data Sharing / Training etc and has this year undertaken the Assessments against the NIS-D Cyber Assessment Framework, the Cyber Essentials plus requirements, the NCSC Board toolkit and ISO27001.	A10.a) Information Governance Champions were discussed at the July Information Governance Group and Digital & Data Committee and will be considered as part of the review of the new Operating Model to ensure roles are identified as appropriate within new structures. In line with the 2021/22 Internal Audit Plan for Cwm Taf Morgannwg University Health Board Internal Audit undertook a review of the arrangements in place for the completion of the Information Governance (IG) Toolkit resulting in Substantial Assurance being received. This will be reported to the Audit & Risk Committee in August 2022. In May 2022 after reviewing and streamlining the NIIAS process from an IG perspective, the team were able to restart the monitoring of own record and commence monitoring of family record accesses on the 1 May 2022. This allows the team to identify themes and learning and target training as appropriate. An updated cyber improvement plan which incorporates data protection has been agreed with the WG Cyber Resilience Unit. This adopts the NIST framework and on an asset by asset and system by system level prioritised by criticality seeks to get the UHB to a far better degree of cyber and protection resilience, using the CIS controls as the basis. In addition we have strengthened our automated controls using Lansweeper to monitor servers, switches and firewalls and solarwinds and avant & TrackIT for endpoints and are enforcing the automated patching of assets using Solarwinds, Avanti & SCCM. Further use of automated controls to protect data leakage over and above MailMarshall for email are being taken forward for the MS 365 suite on a national level and within UHB we are looking to determine what we can do	**A10** (medium): We require further information about how the Health Board is monitoring compliance with DP policies and procedures across each locality and department rather than just at an organisational level through the completion of the annual IG Toolkit assessment.	No progress - organisation working through the high priority actions, which predominantly affect the whole organisation due largely to the design of the NHS Wales data and infrastructure architecture	No progress

A11	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	Accept	KPIs are a standard agenda item Health Records has now been added as a standard agenda item from March 2022. This routine report will include incidents, risks and case note availability. Ongoing, these indicators will be reviewed routinely to ensure they remain fit for purpose.	A11.a) **Complete** - a Medical Records Report is now received as standard at the Information Governance Group.	Completed		
A12	Performance to IG KPIs is reported and reviewed regularly.	A12. See above	A12. See above	Medium		See above	A12a -**Complete.** KPIs is a standing agenda item on the IG Group.	Completed		
A13	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	Accept - partially	Due to the limited resource within the IG Team, we accept that we are not in a position to retrospectively review agreements in place where we are the Lead party. Whilst the WASPI central team issue quarterly reports we accept that this is a risk. This is on the risk register. The information sharing register is presented at every IGG for information which includes all CG approvals. We will continue to ensure that all new processor agreements accurately record the intended data flows & that these are established before any systems are implemented. In conjunction with the requirement to update and improve the asset register, which incorporates medical device discovery, undertake a process for identifying existing processor arrangements & where these lack adequate contractual arrangements and records of flows take actions for these to be established. We will explore the ability to use Cyber and firewall monitoring software to identify the outbound flow of data – which will inform discovery. We will continue to contribute to the all Wales (NHS) approach to documenting the flow of data from within national systems We will undertake an audit , leading to an update of the integrated asset register, business continuity and disaster recovery entries.	The majority of the sharing of the patient record for direct care purposes is covered by the NHS Wales control document. A copy of which is provided. The Health Board is reviewing the DPIAs that were undertaken nationally and has completed the mapping of data from the warehouse (our central returns which account for a sizeable proportion of our flows).	Not started - A13 (high): Evidence provided focuses on the Welsh Control Standard which covers controller to controller data sharing. We require evidence to show what measures have been introduced to track and record all data flows, and as a result how the Health Board has assurance that all data processors are bound by an appropriate contract. We have How do we document our processing activities? guidance on our website that the Health Board may find helpful.	Focus has remained on areas where new or upgraded data sharing and clinical applications are being put in place. Band 3 is working through the legacy issues.	DHCW have provided updated documentation on data sharing for systems they manage on behalf of NHS Wales. No progress on working through the legacy processor agreements
A14	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	Accept	The procurement process is being reviewed at an all Wales basis, given the increasing use of cloud. The UHB will ensure that the requirements of the DPA legislation are incorporated within the new process.	Third party and supply chain management is recognised as an area for improvement for the Health Board and the wider NHS in Wales. A schedule of improvements applying the NIST framework has been adopted which incorporates in stage 3 supply chain management.	Not started	No progress	No progress
A15	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	Accept	In addition to the actions identified in A13, a questionnaire will be issued to all staff asking them to identify what personal data they use and store, where it is stored and whether it is shared.	A large number of our clinical systems and assets managed by the central digital team have now been added to the asset register and the organisation is starting to draw together the information asset register, service catalogue, disaster recovery, business continuity and other useful information into one location on a SharePoint site. This is an agreed and prioritised objective for the digital team and all technical heads are actively contributing. In respect of assets out with the corporate teams' direct management we are presently well into our migration of data of personal folders into the cloud. As part of this exercise all members have been asked to cleanse the data they hold. A second outcome has been that additional assets have been identified, which has led to consideration as to how best to manage this data - for protection and clinical use. The Health Board is combining the asset register with the digital programme catalogue and DC/BR arrangements to create a comprehensive		Focus predominantly driven through enhancement of the product catalogue for the cyber improvement plan and the critical assets	IG officer leading review of the ROPA, but only commenced end of February 2023
A16	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	Reject	The HB does hold a register for sharing activities by way of a database, and a Information Asset register on SharePoint. In addition to this. The detailed data sharing activities is captured in the DPIA / agreement whilst the system details are held in the IAR. We are reviewing options as to how these can be linked & expanded to include disaster recovery and back up arrangements.	Completed and previously shared.	Not started - A16 (high) and A17 (high): We require evidence to show that the Health Board has a formal, documented and comprehensive record of processing activities (ROPA) in place that meets UK GDPR Article 30 requirements. The Health Board may find it helpful to review the ICO's ROPA guidance when implementing these two recommendations.	No change	IG officer leading review of the ROPA, but only commenced end of February 2023
A17	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	Partially accept	The IAR contains the legal basis for which a system processes data. The supplementary agreements required will also contain the legal basis / method / duration etc however these are two separate registers as opposed to one central one.	Completed and previously shared.	Not started - A16 (high) and A17 (high): We require evidence to show that the Health Board has a formal, documented and comprehensive record of processing activities (ROPA) in place that meets UK GDPR Article 30 requirements. The Health Board may find it helpful to review the ICO's ROPA guidance when implementing these two recommendations.	No change	IG officer leading review of the ROPA, but only commenced end of February 2023
A18	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	Accept	The HB has a privacy notice in place and it is available via the website and intranet. We will undertake a review of the notices to ensure they are clear. We have added the retention schedule on to the section where the privacy notice is.	Completed. Notices have been reviewed and published on the Health Boards Website.	**A18** (high): The Health Board's website privacy notice has been updated to include more detail on the rights of the data subject. However, from the evidence provided, the Health Board has not implemented all aspects of the recommendation and we note the privacy notice still has insufficient information about the types of personal data collected and the purposes for processing, and there is very limited information about retention periods.	Updated privacy notice drafted and being prepared for release (formatting/translating etc)	Complete

A19	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 the 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	Partially accept	The issue regarding other languages will be raised with the Equality Team. Where there is a specific request, we currently translate as required but will consider what we can routinely make available. As explained, the website has recently been amended and the changes were not discussed with IG. This is being picked up with the comms team to ensure our privacy data is reverted back to its own section, clear to find and is in one notice as opposed to the tabs they are currently under.	A19.a) Where there is a specific request, we currently translate as required but will consider what we can routinely make available. A19a) Complete. Notices have been reviewed and uploaded to the website including children's privacy notice.	**Not started - A19** (medium): **a**. We require written assurance to confirm what additional action the Health Board has taken to make privacy information routinely available in languages other than Welsh and English; **b.** We require commentary to explain what changes the Health Board has made to its website privacy information to ensure that it is presented in a way that is clear for users to follow and find the required information. Additionally, the action plan says that the children's privacy notice has been reviewed and uploaded to the website but upon review by the ICO the children's privacy notice states that it was last reviewed in January 2020.	No progress	Not intending to progress
A20	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	Partially accept	There is Policy on Policies within the HB and the IG policy schedule is a standard item of the IGG. All policies / procedures in place are available on SharePoint. The DPIA process has been built into the Project Board and a recent message has been sent out to all staff regarding DPIAs. We are considering adding the DPIA form into the overarching Policy on policies.	A20a) the Assistant Director of Governance and Risk will link in with the incoming Head of IG to update the 'Policy on Policies' to reflect the need for policy authors to consider the requirement for a DPIA where applicable.	**Not started - A20** (low): We assess this recommendation as 'not started' as the commentary indicates that the incoming Head of IG will be jointly tasked to review relevant policies, and the role has not yet been recruited to.	Operational requirement which is being baked in to custom and practice	Policy on policies not yet updated
A21	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	Accept	Our DPIA policy includes a review date however we have strengthened the wording within the template regarding the requirements.	A21a) The DPIA document included a review date however it has since been strengthened to ensure that the narrative accurately reflects the requirements to review.	**Not started - A21** (medium): Whilst the DPIA template has been updated to include a reference to the requirement to review a DPIA regularly, commentary does not indicate that the DPIA procedure has been amended to address this recommendation.	No progress	No progress

Accept	Not started
Partially accept	In progress
Reject	Completed