ion 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	Implementation Date	Owner	Update at 6 months (August)	ICO Officer's feedback - August 2022	November 2022 update	February 2023 update
B01	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	Accept	The Health Board agrees with this recommendation and will look to appoint a Deputy Caldicott Guardian. In the absence of the Caldicott Guardian, the IG Team would approach the SIRO / DPO / CCIO / Safeguarding lead or Medical Director depending on the nature of the request. We look to include the approved procedure into HB guidance for staff and on the IG section of the website with contact points.	May-22	Director of Public Health	B01a) The Executive Medical Director has been nominated as Deputy Caldicott Guardian. B01.b) The Health Board is developing a policy to support the sharing of personal information in the event of an emergency or critical situation that will complement existing data sharing policies within the Health Board.		Arrangements to replace the Caldicott Guardian being resolved at meeting of MDs & AMDs on 6th December. Both MD and CCIO have stepped in to date.	Medical Director confirmed as CG, CCIO as the Deputy CG.
B02	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	Accept	A Training Needs Analysis is being considered to include key roles where specific training is required. Due to constraints with capacity, we are taking a risk based approach to offering training routinely.	Oct-22	Director of Digital	Induction of clinical staff continues to include data protection and cyber security. However Specific matters relevant to clinicians such as safeguarding and sharing information with the police & other agencies are being incorporated as part of a revised curriculum in readiness for the new round of induction starting on 8th September 2022. On commencement with the Health Board all employees will undergo and induction and will receive key policy documents.	**B02** (high): Whilst good progress has been made on the provision of data sharing training to relevant staff at induction when they join the Health Board, we require evidence to show that the Health Board has identified and delivered specialist training to existing staff that are likely to make decisions about data sharing.	No progress - proposing to tie this in with launch of new cyber module and linking it with access controls (NADEX IDs) - with WG & expected 23/24	No progress
B03	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	Accept	The DPO is currently reviewing the privacy notices as HBs adopted the All Wales notice that was approved. We will ensure that the legal basis we can rely upon are listed.	Mar-22	Data Protection Officer	B03.a) Complete - This has been amended on the Health Board's website as this was an was oversight in the way the website was laid out.	**B03** (high): Whilst some broad information about data sharing has been added to the Health Board's website privacy notice, more work is needed to ensure that data subjects are sufficiently informed about what data may be shared with other organisations and the lawful basis being relied on to share data. Current privacy information tells individuals that their data may be processed with their consent, which in practice is unlikely to be the lawful basis being relied on to process personal information for direct care purposes.	Privacy notice is in the process of being updated and translated into Welsh	Privacy notice further updated
B04	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	Accept	We have reviewed the DPIA template and consider that the assessment does include criminal data in Section C , Part 1. There is the opportunity for this box to be selected along with other special category data and that of a higher sensitivity. In addition to this, the template requires the legal basis for processing to be confirmed under Section C part 1 (question 2). We have reviewed the ICO DPIA sample template and consider we have covered all the requirements. We would be grateful for further advice on this element. In addition to this, any information sharing agreement would require all data shared to be listed in detail. along with the justification as this is included routinely in them templates.	N/A	Data Protection Officer	We have determined that on the very rare occasion where we do process criminal data and the box that is available is ticked we will trigger additional processes to ensure compliance with the legislation. An extended version of the DPIA template incorporating the requirements for criminal data processing is being prepared.	B04 (medium): Where the Health Board relies on UK GDPR Article 6(1)(e) (public task) to process personal data, it should be able to specify its relevant task, function or power, and identify its basis in common law or statute. Where special category data is shared the Health Board should ensure that in addition to identifying a UK GDPR Article 9 condition for processing that it also, when required, meets any additional conditions or safeguards set out in UK law in Schedule 1 of the DPA 2018. Where criminal offence data is shared the Health Board should ensure that it can identify a specific condition for processing in Schedule 1 of the DPA 2018. For accountability and transparency purposes, the assessment of the legality of each data sharing activity should also be sufficiently documented. The DPIA template seen by the ICO during the audit does not allow for the inclusion of Schedule 1 DPA 2018 conditions for the processing of criminal offence data, or for special category data when this is required.	no change	Policy was agreed at IGGroup. The DPIA will include the ICOs recommendations for processing schedule 1 data

B05	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	Accept	A central register is in place and we have taken a risk based approach due to capacity constraints where possible to ensure there are appropriate agreements in place. The IG team have built a review date into the central register to ensure they are monitored and signed off by all parties.	Apr-22	Director of Digital	Overarching control document has been updated and signed by all users for provision of direct care. This sets the standards and requirements for sharing the electronic patient record across appropriate Welsh organisations and mitigates the risk and makes clear on the required specifications of partners we are sharing data with	**Not started - B05** (high): Whilst we agree that this recommendation is 'not started', commentary focuses on data sharing arrangements that come under the Welsh Control Standard for direct care purposes. The Health Board should also consider what action it will take to ensure that other routine data sharing activities outside the Welsh Control Standard are covered by appropriate agreements (e.g. data sharing for purposes other than direct care such as research, or data sharing with organisations that do not participate in the Welsh Control Standard).	Legacy data sharing	No progress
B06	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	Partially accept	The IG team have reviewed the data sharing templates and consider that they do allow for the consideration of special category / sensitive data and partner responsibilities. The ISP, DDA and ISA agreements have been adopted on an All Wales basis. However, as FOIA is not included this will be raised with the central WASPI team for them to consider if this can be included.	Apr-22	Director of Digital	The ISP, DDA and ISA agreements have been adopted on an All Wales basis. However, as FOIA is not included this will be raised with the central WASPI team for them to consider if this can be included. A request to WASPI has been made and awaiting outcome.	**B06** (medium): We would assess this recommendation as 'in progress' as the Health Board has contacted the central WASPI team to see if FOIA requirements can be included in WASPI data sharing templates. However, the Health Board also needs to ensure that it implements the recommendation for data sharing agreements to meet legislative requirements for any sharing activities that are covered using non-WASPI templates.	No update from the WASPI team	Wales Accord on the Sharing of Personal Information (WASPI) framework being updated in order for signatories to apply for it to become an approved Information Commissioners' Office (ICO) Code of Conduct . Schedule 1 conditions will be incorporated within DPIA
B07	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	Accept	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 not the Lead party. Whist 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.	Sept - risk based approach	Data Protection Officer	Position is as noted in March 2022. Progress has been made on documenting and reviewing data sharing arrangements actioned via the Information Governance Team.	**Not started- Noting: B07.a** (high): The recommendation to review sharing agreements has not been started due to the current resourcing issues within the IG team and commentary states that the risk is included on the risk register. We would expect that as soon as resourcing levels permit, the Health Board should implement a process to ensure all data sharing agreements are regularly reviewed on an ongoing basis.	No progress	The IG team are conducting an audit of all existant sharing agreements. Some have now been completed , Others are still sharing so review date have been checked and updated. There are a number from 2021 whereby the lead name on the spreadsheet no longer works for the organisation etc which are being diverted to other members of their department. No progress has been made in providing oversight of higher risk agreements at this time
B08	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	Partially accept	The IG Team has a central log for information sharing agreements. This includes DDA, ISPs, ISAs etc. However additional columns have been added into ensure copies of approvals are retained alongside review dates. This is presented routinely as a standard agenda item at IGG.	Mar-22	Data Protection Officer	Completed and centralised register previously provided to Auditors.	**B08** (medium): At the time of the ICO audit in February 2022, we observed that there were several separate repositories for data sharing agreements within the IG file directory. Whilst commentary says that the IG team has a central log for information sharing agreements with additional fields, we require further detail around any measures that have been taken to review and 'weed out' older lapsed or expired agreements that may be held outside of the central log.	We have commenced a review of the exisitng data sharing agreements where no review date was initially documented	As above, the audit of all sharing agreements is intended to weed out those that have expiered and ensure those that are ongoing contain accurate up to date information
B09	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	Accept	Retention periods are included within standard templates and the DPIA template however we accept we do not undertake routine checks. We have had to adopt a risk based approach to this and the issue of resource is being addressed at an Executive level. Retention would be the responsibility of all parties based on the types of data that this involved. All parties are responsible for considering their own data retention and handling of any data entrusted to them, i.e. Data Controller, Processor or Third Party (normally under the Data Processors own arrangements) that they would be responsible for any issue or process relating to the data with their own internal controls and if the data was of a common theme (i.e. recruitment, commercial or other data category, that they would apply their own retention and destruction policy to remove data no longer required or of no further legitimate business need from their systems	Jun-22	Director of Digital	Mitigation of this risk is as indicated in March 2022.	Not started - B09 (high): The Health Board says that retention periods are included within standard templates but that it does not undertake routine checks around the retention of shared data by its sharing partners and data processors due to resourcing issues. Data processors in particular should not be expected to apply their own retention periods where they are processing data under instruction from the Health Board. Our guidance on end-of-contract provisions provides further information about this. Specific retention periods/disposal arrangements should be stated within each data processor contract and we have recommended that the Health Board should implement measures to ensure they are being adhered to in practice. These could include obtaining a certificate of destruction/return of shared data at the end of the contracted period. As above we would expect that as soon as resourcing levels permit, the Health Board should implement a process to ensure that shared data is not retained by sharing partners and data processors for longer than is necessary.	IG administrator will commence this work, in Decemeber 2022	No progress

B10	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	Accept	Retention periods are included within standard templates and the DPIA template however we accept we do not undertake routine checks. We have had to adopt a risk based approach to this and the issue of resource is being addressed at an Executive level. All parties are responsible for their own data handling/confidentiality/access/use arrangements and that as a procuring organisation, we wouldn't be vicariously liable for another company, contracted under an NWSSP contract if they have a data breach but they would in fact, have their own IG arrangements in place and should routinely report any breaches. In relation to system access, detailed information access and audit responsibilities should be written into a DPIA. One of the recommendations dependant on the service is to ensure that a specific list of personnel are responsible for any	Risk based approach Nov 2022	Director of Digital	The Health Board has adopted the NIST framework, we have agreed a cyber and protection improvement plan which places a priority on secure use of administration privileges, secure configuration (include access configuration) , monitoring of audit logs and vulnerability management - this is focussed on our top 20 critical systems and will be a rolling programme. In regards system access the Health Board has recently made funding available for 2 additional asset management posts to strengthen access control. This has involved a significant review of authorised users. A process is in place that enables active and ongoing management led by the Head of End User Computing.	**B10** (high): Commentary and evidence presented outlines the measures that the Health Board has taken to strengthen detective access controls on its own systems that can be accessed by sharing partners. However, we require evidence to show that the Health Board has measures in place to provide assurance that its sharing partners have implemented robust access controls where access to shared data cannot be directly monitored by the Health Board e.g. where personal data is shared outside of a shared system or platform.	No progress	NHS code of connection exists.
B11	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	Accept	Whist the data sharing agreements include a standard clause that all parties are expected to have an assurance framework and appropriate policies in place, the HB does not routinely seek assurance that this has been implemented.	Nov-22	Director of Digital	The Welsh Control Standard for Electronic Health and Care Records which articulates the overarching requirements for assuring data controllers that there partners in care provision across NHS Wales are compliant with data protection legislation has been recently updated.	**Not started - B11** (high): We require evidence to show that in addition to clauses or terms contained in sharing agreements, the Health Board is seeking separate assurances that its sharing partners (both within and outside the Welsh Control standard) have implemented effective incident management procedures including defined incident reporting deadlines.	No progress	NO progress - the UHB is carrying a known risk in regards to supply chain management - Addressing this will require additional manpower.
B12	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	Accept	The subject access procedure is under review and we are looking to add a process for ad hoc personal data requests and third party data requests. This will include working with Health Records and other departments to ensure a consistent approach	Jun-22	Director of Digital	Completed - Personal Data Request Procedure approved in July 2022.	**B12** (high): We are satisfied that there is now a single documented procedure in place for responding to ad hoc third-party requests for personal information but require additional information to show how the Health Board is ensuring that all relevant staff are aware of the new procedure and that this is being followed in practice.	We can not provide this evidence	We can not provide this evidence
B13	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	Accept	As above (B12)	Jun-22	Director of Digital	Complete - Personal Data Procedure Approved in July 2022.	**B13** (high): We require evidence to show what mechanisms are now in place to track and monitor ad hoc third-party requests for personal data, including keeping records of responses, approvals and quality assurance against legislative requirements, and how these mechanisms are being used to provide sufficient senior oversight about the quality of how such requests are being collectively handled across the Health Board.		Significant step backwards following loss of the team and organisational change
B14	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	Accept	The HB will look to implement a policy / procedure to include bulk transfers of personal data. The All Wales File Sharing Protocol is stipulated as standard on all new data flows where secure APIs are not in place.	Sep-22	Director of Digital	The use of Welsh file sharing protocol remains a stipulation and is used by the corporate team where secure APIs do not exist. Mail Marshall has put in place automated controls to filter out any transfer of PII via email. DHCW on behalf of NHS Wales are looking at something similar for data leakage prevention via MS 365. The Health Board is looking at options for automating the identification and management of PII flows through our firewalls. DPIAs are being put in place and adhered to for the bulk transfer of medical records (e.g. to our scanning partner).	**Not started - B14** (medium): We require commentary to specifically address the recommendation that there should be a sufficiently detailed policy or procedure in place to cover bulk transfers of personal data.	No progress	To be addressed via national review of policies led by IGMAG.