Agenda Item	7b

Freedom of Information Status	Open	
Reporting Committee	Information Governance Board (IGB)	
Author	Sian Richards, Interim Deputy Chief Information Officer	
Chaired by	Pam Wenger, Senior Information Risk Officer (SIRO), Director of Corporate Governance	
Lead Executive Director (s)	Pam Wenger, Director of Corporate Governance	
Date of last meeting	18 September 2018	

Summary of key matters considered by the committee and any related decisions made.

- **Caldicott Principles into Practice (CPiP) –** CPiP is a national annual assessment tool, the results of which are published externally. ABMU achieved 91%, which brings it into the highest assurance assessment tier for the first time, this reflects the improvement in information governance (IG) during the last financial year.

- **General Data Protection Regulation (GDPR) Compliance –** GDPR came into force in May 2018. A detailed Work Plan is in place and on target to complete the required actions within the agreed timescales of December 2018 for the majority of actions and May 2019 for nine longer term more complex areas. The resources given to the IG team in 2018 have been fundamental in achieving the improvements and enabling this notable turnaround from the concerning position reported at the start of 2018.

- **Information Asset Register (IAR) –** GDPR requires organisations to have an IAR. The IAR is a catalogue of the information the organisations holds and processes, detailing where it is stored, how it is moved around and how it is shared. The IAR is legally required in order to provide adequate assurances that information assets are being processed legally, risk assessed and managed accordingly. An IAR is a live document, with responsibilities assigned to Information Asset Owners (IAOs) across the Health Board. Currently it has 1651 assets noted, with approximately 50% containing complete datasets. Work is ongoing to complete asset identification, logging associated information on each asset and managing all associated risk. Details of compliance by SDU and corporate department were reported to IGB. IGB leads were asked to continue with plans to improve content and quality of the IAR.

- **National Intelligent Integrated Auditing Solution (NIIAS) –** This is a software auditing tool available to all Health Boards / Trusts across NHS Wales. It is used to detect potentially inappropriate access to electronic clinical records, where employees may have viewed data they are not entitled to as part of their official duties. Parameters checked are access to one's own clinical record, and inappropriate access to a family member's record. The Disciplinary Policy is followed for the latter. ABMU utilise NIIAS weekly and follow up on actions necessary / taken, alongside Workforce & OD. The Health Board's figures are very low compared to many other Health Boards with only 8 instances of confirmed inappropriate access to family member records since the last IGB in July.

- **Senior Information Risk Owner (SIRO) Report –** the SIRO Report has been drafted and sent to the Health Board for approval in November. It reports ABMU's position with regards to IG, Data Quality, Cybersecurity, Clinical Coding and Health Records. The expectation is based on the initial feedback from Audit Committee in September, that it will be as well received as last year's inaugural SIRO report. It provides good assurances on information security and governance. Not all Health Boards choose to publish a SIRO report so the ABMU position is one of good practice.
- **Cybersecurity –** To improve the cybersecurity controls in place across the Health Board detailed work plans have been implemented with regards to patching of systems and servers, licencing and software asset management. A key development in the period is the adoption of the National Cloud Guidance for services looking to transfer their information to cloud servers. External consultants, Stratia, have produced a report on ABMU's IT security weaknesses and an action plan is in place to address these areas.
- **Welsh Audit Office (WAO) Structured Assessment –** WAO completed its audit of IG and the verbal feedback was that ABMU is outperforming most other Welsh Health Boards in most areas of data protection practice, whilst recognising the work still to be done to become fully GDPR compliant. The formal report is awaited.
- **RFID –** The Health Records Modernisation Programme will implement a RFID solution, rolled out in 2019, with the objective of improving the clinical and logistical problems of a paper based health record whilst also modernising and improving the Health Records service. The solution will provide RFID tagging of acute records, Location Based Filing using barcode scanning and identification of a patient's record's location via fixed sensors. This will enable the record to be easily tracked, located and made available when required.

Key risks and issues/matters of concern of which the board needs to be made aware:

- **Mandatory IG Training Compliance –** Training compliance was noted at 32% in March 2017. Following a drive to proactively target non compliant staff (including students, volunteers etc), compliance now stands at 74%. There is a requirement for compliance to be at 95% and work continues to further improve staff completion of the mandatory training. A commitment has been given to WAO to considerably increase ABMU's IG training compliance by the end of 2018; the progress and improvement is evident but further work is required to achieve the 95% target. Detailed compliance reports are sent to every IGB lead on a monthly basis to proactively encourage local improvement.
- **Infected Blood Inquiry –** This was officially established by Parliament in June 2018 and a directive has been received to immediately suspend the destruction of all relevant corporate and health records. As this Inquiry relates to records created in the 1970s and 1980s it should be noted that some have already been legally destroyed. Following a directive from Andrew Goodall, Welsh Government the Health Board has ceased destruction of all corporate and health records indefinitely. Some departments manage their own destruction and there is a risk that not all departments are aware of the destruction embargo, this is being mitigated with ongoing communication. Within Health Records the major impact is the increased need for storage on a long term basis. Since August there are already 1200 boxes of records that could have been destroyed that are now being retained. As a result additional storage is being sourced.
- **Subject Access Requests (SARs) –** Under GDPR, individuals have the right of access to their personal information, commonly referred to as subject access requests (SARs). This gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why their data is used. Under GDPR the timescales to comply with SARs have reduced and no charge can be made, which has resulted in a loss of revenue of around £170k pa. The department has experienced

a 12% increase in SARs received. The response compliance rate will be monitored to review the impact of the increase in requests.

- **IG Breaches –** IGB are made aware of all breaches, 7 of which have been reported to the ICO since May 25th when the potential fine per breach was raised from £500k to approximately £48m. Breach reporting has become mandatory, while the threshold for reporting is still under review with the ICO. All breaches are being actively managed by IG and relevant departments, and no decisions from the ICO have been received to date. The ICO and WAO have verbally recognised ABMU's robust breach procedures and reporting practices.

- **IG Audits –** Going forward approximately 8 planned IG audits plus audits following notable breaches are taking place across the Health Board per month. Currently IGB are aware of 2 red audits, 7 yellow and 5 green since February 2018. The main area of concern is the breach of records at Gorseinon reported to the ICO in June. Whilst plans have been agreed to remove the records to alternative locations, Medical Human Resources Records documentation and Cardiology CDs still remain at the site against IG advice. This has led to a delay in the required follow up report being sent to the ICO. Audits have flagged a number of other unsuitable areas also being used for archiving of sensitive personal data, these are being managed through detailed improvement plans and reporting.

- **Contracts –** There are unknown contracts signed with 3rd parties without IG or Procurement support that are highly unlikely to be GDPR compliant and likely to result in ICO scrutiny in the event of a breach. Their existence is being actively sought by both IG and Procurement to address and mitigate the risk.

- **Cybersecurity resourcing –** The resources available to provide adequate assurances that ABMU is complying with Cybersecurity requirements is being reviewed and opportunities explored to increase the resources in this area.

Delegated action by the committee:
No delegated action was taken by the committee at this meeting.

Main sources of information received:
- Caldicott Principle in Practice Outturn Report - IG Update Report - GDPR Readiness Reports and Action Plan - IAR Report - Health Board IG Risk Register - IG Key Performance Indicators - Health Records Report - Cybersecurity Report - IGB Lead Progress Reports - Fax Usage Report - Data Quality SBAR - All Wales IG/Security/Email/Internet Policies and ABMU IG Procedures - Infected Blood Inquiry documentation - Welsh Clinical Portal – Medicines Save – Root Cause Analysis

Highlights from sub-groups reporting into this committee:
No sub-group reports to note

Matters referred to other committees
No matters were referred to other committees at this meeting.

Date of next meeting	20 November 2018