Agenda Item	6a
Freedom of Information Status	Open
Reporting Committee	Information Governance Board (IGB)
Author	Becky Wadley , Head of Information Governance
Chaired by	Matthew John, Chief Information Officer
Lead Executive Director (s)	Pam Wenger, Director of Corporate Governance
Date of last meeting	12 February 2018

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

- **General Data Protection Regulation (GDPR) Compliance –** GDPR came into force in May 2018. The detailed Work Plan has been formally closed by IGB, having completed it ahead of target within the agreed timescales of December 2018 for 51/59 actions, and Summer 2019 for the remaining eight longer term more complex areas. These eight actions have been added to the IG Strategic Work Plan 2019-20 which was brought to IGB for comment.
- **Policy Development -** The ABMU IG Procedures, all Wales IG Policy, all Wales Internet Use Policy and all Wales Email Use Policy have been approved by IGB and the Executive Team, and are being taken to the Local Partnership Forum in March 2019 for final approval. A bulletin will then be issued, and the IG intranet pages, the policy acceptance screen and face-to-face training presentation will also be updated accordingly. The Media Handling Procedure, drafted by the Communications Department, was approved by IGB. Comments have been received on the ABMU IT Security and Asset Management Policy and this will be brought to the next IGB for approval.
- **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 1877 assets noted, with 100% now noting legal basis for processing and retention periods. Work is ongoing to complete asset identification, logging associated information on each asset and identifying 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. IAOs will be given direct access to the IAR on SharePoint, rolled out from March 2019; the responsibility for registering and auditing their own information assets lies with them going forward, with the support of any nominated Information Asset Administrators (IAAs).
- **Data Protection Impact Assessments -** Under the General Data Protection Regulation (GDPR), carrying out a Data Protection Impact Assessment (DPIA) is required by law for all significant changes or new methods to process personal data. The requirement applies to high-risk services or systems; this includes the processing of special categories of personal data in the health sector. There are currently 46 entries on the DPIA register, including details of projects that completion of the initial screening questionnaire showed no DPIA was

necessary. IGB Leads were asked to continue to raise awareness of the need for all initiatives to complete the DPIA screening questions.

- **Data Sharing Register** – There are 74 sharing agreements currently on the Register, and this is an area of priority to address (review and expand) during the next financial year.
- **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 15 instances of confirmed inappropriate access to family member records during the period November 2018-January 2019 inclusive.
- **Cross boundary work** – In order to be compliant with data protection legislation, a number of documents have been produced to give suitable assurance: A staff privacy notice and a patient privacy notice ensure legally fair processing; a Data Protection Impact Assessment ensures privacy by design, and; an Information Sharing Protocol ensures legal and secure sharing of patient and staff information between the two Health Boards. Work continues to prepare for the 1st April 2019.
- **Internal Audit Report** – Internal Audit undertook their review of the GDPR Work Plan completed actions in November 2018. The report noted a green Substantial Assurance result. The only recommendation relates to the submission of IGB Lead update reports and this has already been actioned in full.
- **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. External penetration testing took place in January 2019 and the results support the plans already in place with regards to patching requirements. Risks are already reduced via the use of anti-virus software, web and email filter software, scanning on advanced security network equipment and the restriction of user rights to minimise the likelihood of installation of rogue software. The issue of resourcing for Cyber Security within the NHS is under discussion at national level.

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

- **IG Risk Identification Log** – A total of 28 Health Board wide IG risks have been noted and brought to IGB for consideration of how best to mitigate against them. Further discussions are to be held between the Chief Information Officer, the Senior Information Risk Owner (SIRO) and the Data Protection Officer to address this issue.

- **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 reported to February IGB stands at 83%. 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 continue to increase ABMU's IG training compliance; 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, and the IG team proactively email specific departments and non compliant staff. Mandatory training is now available on mobile devices, and a video of the IG mandatory training is due to be filmed in April. Due to lower staffing levels within the IG team, departmental face-to-face training sessions are now only offered in extenuating circumstances.

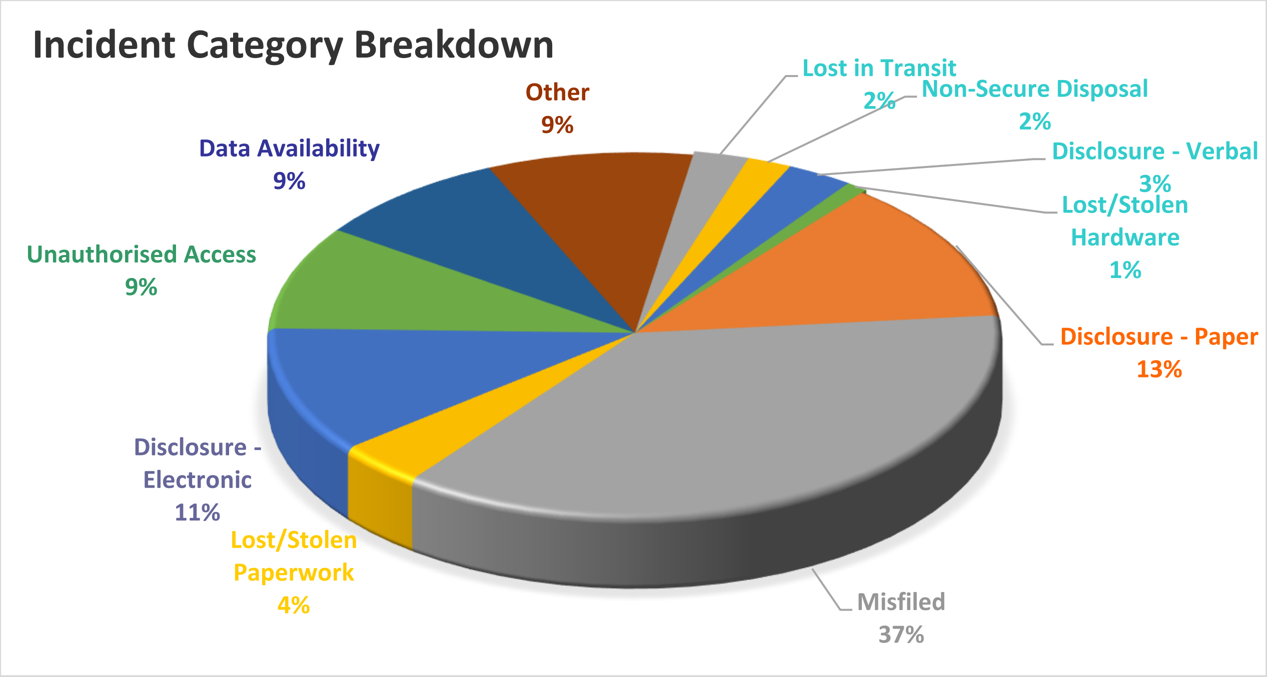
Area	Number of staff in area @ 04.02.2019	Compliance % as it stands on 04.02.2019	Movement from last IGB Reported Compliance %
Corporate Departments			
Board Secretary	37	68	-11
Chief Operating Officer	1640	67	NA
Clinical Medical School	18	94	-1
Clinical Research Unit	42	93	5
Delivery Unit	32	97	0
Director of Strategy	38	84	NA
EMRTS	28	82	-4
Finance	93	89	-4
Informatics	398	94	-3
Medical Director	47	96	0
Nurse Director	80	88	-3
Workforce	143	94	2
SDUs			
Mental Health & Learning Disabilities	2007	91	5
Morriston Hospital	3612	77	5
NPTH	1447	90	2
Primary Care and Community	1720	92	2
Princess of Wales Hospital	1787	84	2
Singleton Hospital	2400	81	8
TOTAL			
Overall Health Board	**15569**	**83**	**9**

- **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. There are already 20,000 clinical records that could have been destroyed that are now being retained. As a result additional storage has been sourced at Unit 32 near Neath Port Talbot Hospital.

- **Records Management –** There have been several instances of records being stored in inappropriate unsecured locations which have been accessed by members of the public. These instances have been reported to the Information Commissioner's Office. The Chief Information Officer has been given the brief to lead on the future storage requirements of the Health Board, and in the meantime the IG team continue to work with Estates to locate and audit records stored in unsuitable locations.

- **IG Department Resourcing** – The Department had two vacancies at the time of the boundary change resource decisions, and the budget for these has been passed across to Cwm Taf. As a result, the IG Department has reduced by 25% with no significant change in workload. Therefore the Department are prioritising carefully to ensure the best data protection compliance possible, but its ability to manage audits and breaches with a suitable level of assurance for the Regulator, the Information Commissioner's Office (ICO), is compromised.

- **IG Breaches –** Breach reporting to the Information Commissioner's Officer (ICO) has become mandatory, while the threshold for reporting is still under review with the ICO and ABMU are in direct contact with the ICO to confirm reporting requirements. All breaches are being actively managed by IG and relevant departments, IGB are made aware of all breaches, 14 of which have been reported to the ICO since May 25th when the potential fine per breach was raised from £500k to approximately £48m. 12 of these have now been closed by the ICO with no penalty but with many recommendations that will be actioned by the relevant departments with the IG team's support. The ICO and WAO have verbally recognised ABMU's robust breach procedures and reporting practices. During the period 1st November 2018 - 31st January 2019, **208 IG related incidents and near misses were reported** onto DATIX. A summary of the DATIX report was shared at IGB for information. There is potential that under the ICO's proposed threshold for reporting, nearly all of these would be reportable, however it is anticipated that an agreement will be reached on a more workable threshold in the first quarter of 2019-20. A breakdown of the incident categories is provided for information in the chart below:



Reported incidents are monitored for trends, common risk themes and any valuable lessons learned are shared with all members of the Information Governance Partnership Group (IGPG), with staff via information bulletins, updates to the IG intranet pages or other available training and communication methods. Consideration will be given to any trends regarding their inclusion on local or Health Board risk registers.

- **IG Audits –** IGB were informed that 36 audits were performed when a dedicated resource was employed within the IG Department. However, now that the team have lost that resource, the audit programme for 2019-20 will prioritise audits performed as a result of an ICO reportable breach, and follow up audits. Currently IGB are aware of 7 red audit reports in total, given to Singleton Outpatients, NPTH/PoW Radiology, Medical Human Resources Morriston, Garngoch (various SDUs/Corporate Depts), Gorseinon Bungalow A (various SDUs/Corporate Depts), Estates and Bridgend Private Clinic.

Delegated action by the committee:

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

Main sources of information received:

- IG Update Report
- GDPR Readiness Reports and Action Plan
- IAR Report
- IG Key Performance Indicators
- Health Records Report
- Report from IG Partnership Group
- IG Risk Identification Log
- Cybersecurity Report
- IGB Lead Progress Reports
- All Wales IG/Security/Email/Internet Policies and ABMU IG Procedures
- Media Handling Procedure
- DPIA Register
- Data Sharing Register

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	14 May 2019