



GIG
CYMRU
NHS
WALES

Bwrdd Iechyd Prifysgol
Abertawe Bro Morgannwg
University Health Board



		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	20 November 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. 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 team continue to make very good progress and there is confidence in achieving the agreed end of year position. The final GDPR Work Plan will be brought to IGB in February for formal closure, alongside the new Strategic Work Plan 2019-20.
- **Policy Development** - The ABMU IG Procedures, all Wales IG Policy, all Wales Internet Use Policy and all Wales Email Use Policy have been finalised and approved by IGB. Executive Team are asked to endorse these policies for final approval before being published. 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 all Wales Information Security Policy and the ABMU IT Security and Asset Management Policy was circulated for comment and will be brought to the next IGB.
- **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 1727 assets noted, with approximately 70% containing complete datasets. 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.
- **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 23 entries on the DPIA register. IGB Leads were asked to continue to raise awareness of the need for all initiatives to complete the DPIA screening questions.

- **National Intelligent Integrated Auditing Solution (NIAS)** – 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 NIAS 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 5 instances of confirmed inappropriate access to family member records since the last IGB in September.
- **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 that the National Service Management Board (NSMB) have recommended to NIMB that NHS Wales organisations review the Cyber Assessment Framework (CAF) and Indicators of Good Practice (IGP) and start to implement systems/controls to meet the requirements of the Network and Information Systems Directive (NIS-D). An initial assessment was presented to IGB, the outcome showed that the Health Board has achieved full compliance in 14 controls, it is partially compliant in 5 of the controls, but non-compliant in 20 of the controls. This assessment will now form the basis of a paper and work plan which will look at the work involved to move the 25 partial and non-compliant areas to full compliance, and therefore improving cybersecurity of the organisation.

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

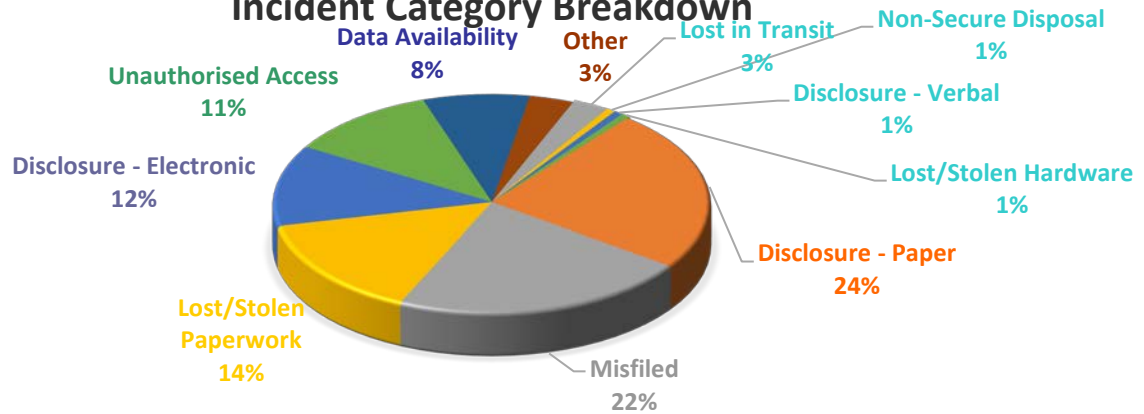
- **Mandatory IG Training Compliance** – Training compliance was noted at 32% in March 2017. Following a drive to proactively target non compliant staff (including students, volunteers etc), compliance reported to November IGB stands at 78%. There is a requirement for compliance to be at 95% and work 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.

Area	Number of staff in area @ 01.11.2018	Compliance % as it stands on 01.11.2018	Movement from last IGB Reported Compliance %
Corporate Departments			
Board Secretary	47	79	-5
Clinical Medical School	19	95	11
Clinical Research Unit	41	88	-7
Delivery Unit	32	97	6
Director of Strategy	1644	56	6
Director of Therapies & Health	24	96	0
EMRTS	29	86	1
Finance	91	93	-1
Informatics	397	97	1
Medical Director	45	96	-2

Nurse Director	67	91	7
Workforce	140	92	-1
SDUs			
Mental Health & Learning Disability	2027	86	5
Morriston Hospital	3629	72	6
NPTH	1441	88	2
Primary Care and Community	1707	90	3
Princess of Wales Hospital	1776	82	4
Singleton Hospital	2386	73	6
TOTAL			
Overall Health Board	15542	78	4

- **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 at unit 32.
- **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, 10 of which have been reported to the ICO since May 25th when the potential fine per breach was raised from £500k to approximately £48m. Confirmation has been received from the ICO that no further action will be taken in two cases, and updates on the other cases are pending. The ICO and WAO have verbally recognised ABMU's robust breach procedures and reporting practices. During the period 1st September - 31st October 2018, **150 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 agreement will be reached on a more workable threshold in early 2019. A breakdown of the incident categories is provided for information in the chart below:

Incident Category Breakdown



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 the audit programme was concentrating on audits as a result of breaches. Currently IGB are aware of 6 red audits (Singleton Outpatients, Singleton DOSA, NPTH and PoW Radiology, Medical Human Resources Morriston, Garngoch (various SDUs/Corporate Depts), Gorseinon Bungalow A (various SDUs/Corporate Depts)), 21 yellow and 7 green since February 2018. Audits have flagged a number of unsuitable areas being used for archiving of sensitive personal data, these are being managed through detailed improvement plans and reporting. It was agreed that this should be added to the risk register.

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
- Cybersecurity Report
- IGB Lead Progress Reports
- Data Quality SBAR
- All Wales IG/Security/Email/Internet Policies and ABMU IG Procedures
- **DPIA 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

12 February 2019