		Agenda Item	**7.2**
Freedom of Information Status		Open	
Reporting Committee	Information Governance Group (IGG)		
Author	Becky Wadley, Data Protection Officer		
Chaired by	Pam Wenger, Director of Corporate Governance, SIRO		
Lead Executive Director (s)	Pam Wenger, Director of Corporate Governance		
Date of last meeting	24 September 2019		

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

- **Membership –** Currently under review to ensure strategic members attend IGG, and operational staff attend the Information Governance Partnership Group (IGPG).
- **IG Strategic Work Plan 2019-21 –** The IGG continue to monitor compliance with data protection legislation via reports, KPIs and scrutiny of the robust Work Plan 2019-21. Completion of the work plan will result in the Health Board having a high level of legal compliance with GDPR and provide good assurances to the Regulator. Some timescales have been amended following a need to reprioritise, based on risk and requirement.
- **Policy Development –** IG Guidance documents have been drafted in various areas of data sharing, Data Protection Impact Assessments (DPIAs) and Privacy Notices. These will be out for comment during October and published in October/November 2019.
- **Information Asset Register (IAR) –** Currently the IAR has 1721 assets noted. The responsibility for registering and auditing information assets lies with Information Asset Owners (IAOs) with the support of any nominated Information Asset Administrators (IAAs). As part of the reprioritisation of the Strategic Work Plan, the IAR will not be proactively expanded by the IG team for at least the next three months; IAO/IAA guidance has been issued and support will be given on request.
- **Cybersecurity –** IGG were presented with a cyber update, including details of the plan to move to Office 365. When this happens it is likely that Access databases will only be supported for a further 3 years so SBU will identify current usage of such databases (utilising the IAR in the first instance) and make alternative arrangements with regards to data currently stored in this format. A Cyber Security manager is currently being recruited to lead development of plans and implementation. There is a cybersecurity training module on ESR which has been publicised, and consideration will be given as to whether it needs to be mandatory for staff to complete. Two Security based policies will be circulated for comment from IGG members before the next IGG in December 2019.
- **Data Quality** – The report summarised the overall performance of the Health Board against the range of indicators that are currently measured for the validity of the Admitted Patient Care dataset, with ABMU/SBU achieving 100% compliance for these standards over the last year. A total of 277 checks are now in place for the validity and consistency indicators. As of May 2019, SBU met the required target for 272 of these checks, achieving 98% overall.

- **Caldicott Principles into Practice (CPiP) Annual Assessment** – This was completed with a score of 94%, up 3% from last year. This is an excellent score, in the top bracket available, evidence of the continued ongoing improvement in IG and Security practices across SBU.

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. 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. IG risks are currently managed via the IGPG to ensure a consistent approach across SBU.
- **Mandatory IG Training Compliance –** Training compliance reported to September IGG stands at 85% (details available in Appendix 1). There is a requirement for compliance to be at 95% and work continues to further improve staff completion of the mandatory training. There is now an IG video available (via the Intranet and network drive) as an alternative to ESR based e-learning to gain mandatory IG training compliance – uptake has been good and very positive feedback received. This is to be translated into Welsh to enable the video to be uploaded onto YouTube to capture those without access to ESR based elearning or the intranet, e.g. Agency workers, new starters, locums, students, volunteers, etc. The requirement for face to face training, currently on hold, is reviewed on a monthly basis.
- **Data Protection Impact Assessments (DPIAs) –** There is a legal requirement to complete a DPIA whenever there is a new use of personal data being considered, e.g. a new information flow, a new system or service. This requirement has been incorporated into both Procurement and Informatics processes, amongst others, but it is yet to be fully embedded across the organisation and several new initiatives have taken place without a DPIA. Work will be prioritised in this area going forward, and a report taken to the next IGG in December.
- **IG Breaches –** Since the new data protection legislation in May 2018, 21 IG breaches have been reported to the regulator, the Information Commissioner's Office (ICO). Of these, 3 were reported since the last IGG in May 2019. To date, 18 have been closed by the ICO and their recommendations taken forward via the IGPG. Between 1st May – 31st August 2019, 162 IG related incidents and near misses were confirmed on Datix. Incident trends are monitored and managed via IGPG. SBU have led on the national development of a breach management process and scoring threshold in conjunction with the ICO.
- **IG Dept Audits –** There is a requirement under data protection legislation to be able to offer documented assurance that an organisation is compliant with the legislation. Therefore the IG Department audit areas across SBU against IG parameters, any risks identified are managed accordingly and formal scheduled follow ups take place unless a Green result was obtained in the first instance. Priority is given to auditing those areas that have suffered an ICO reportable breach, or if a concern has been raised internally. Details of audits that have taken place since the last IGG are available in Appendix 2.
- **IGG Lead Updates –** There is a sub group of the IGG, the IG Partnership Group (IGPG), that receives update reports from all SDUs and Corporate Departments. When Internal Audit issued their Substantial Assurance report on compliance against the GDPR Work Plan in November 2018, the only recommendation was that IGG and Audit Committee were made aware of any notable areas that had not submitted an update report. W&OD and NPTH did not submit a report to the last IGPG.

Delegated action by the committee:

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

Main sources of information received:

- IG Update Report and Strategic Work Plan 2019-21 - IAR Report - IG Key Performance Indicators - Report from IG Partnership Group - Cybersecurity Report - 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	10 December 2019