Agenda Item	6.1
Freedom of Information Status	Open
Reporting Committee	Information Governance Group (IGG)
Author	Becs Wadley, Data Protection Officer
Chaired by	Pam Wenger, Director of Corporate Governance, SIRO
Lead Executive Director (s)	Pam Wenger, Director of Corporate Governance, SIRO
Date of last meeting	17 March 2021

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

- **M365 –** A presentation was given on the governance surrounding M365 and IGG was given suitable assurances of the processes, plans and documentation in place.
- **Cybersecurity –** The team are focussing on the development and execution of HB Cyber Security in conjunction with national colleagues. The Cyber Team are working to ensure compliance with the Security of Network & Information Systems Regulations (NIS-D). Achieving compliance will also impact teams other than Cyber Security, including teams across the whole of SBUHB where networked devices fall in scope; such as medical devices, estates/security and supporting infrastructure
- **Policies –** The following policies were agreed, and subsequently approved by Management Board on 21st April:
  1. *The SBU Data Quality Policy.* Revisions are minor and include: Updated terms, links to other policies, clarifications given, inclusion of childrens' right to recording of their contact details.
  2. *The All Wales Information Governance Policy.* Revisions are minor and include: Grammatical, punctuation and syntax changes, along with removal of any duplicated areas covered.
  3. *The All Wales Information Security Policy.* This replaces the SBU Information Security Policy, working in tandem with the IG Policy (#2 above) and the SBU Cyber Security Policy (#5 below), and has been approved by the Wales Information Governance Board and national Staffside. It provides a high level policy on expectations around secure access, transport, storage and disposal of information.
  4. *The All Wales Internet Policy.* Revisions are minor and include: Updated prohibited email providers and updated guidance on secure internet connection methods.
  5. *The SBU Cyber Security Policy.* This complements the All Wales Information Security Policy (#3 above) by providing technical detail for safe, secure and resilient use of digital services on top of IG regulatory compliance.
  6. *The SBU Health Records Policy.* Revisions are relatively minor and include: Grammatical, punctuation, typo and syntax changes, clarifications given, new sections on destruction, information sharing, Datix and clinical trials, and expansion of staff responsibilities.
  7. *The SBU Compilation of Health Records Policy.* Revisions are minor and include: Updated terms, renumbering of sections, adding page numbers.

Audit Committee – 18th May 2021

8. *The SBU Health Records Tracking Policy*. Revisions are minor and include: Updated terms, grammar and typo changes, addition of untracked record risks and RFID.
9. *The SBU Storage and Security of Health Records Policy*. Revisions are minor and include: Updated terms, grammar changes, page numbers added, clarifications made.
10. *The SBU Retention and Destruction Policy*. Revisions are minor and include: Updated terms and several references to the Infected Blood Inquiry / record destruction embargo.

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

- **Organisational IG Issues/Risks** – These are summarised below, in priority order:
  1. Subject Access Request (SAR) procedures, including redaction (for patients and staff)
  2. Data Protection Impact Assessments (DPIAs) – not having them at all, having them but not being robust enough, not being reviewed, risks not adequately mitigated
  3. Respecting data subjects' legal rights in general (e.g. privacy notices)
  4. Data sharing agreements and contracts
  5. Proactive IG audits – internal planned audits / 3rd party audits

  All mitigating actions possible have been taken, and resourcing is now being assessed. A Task and Finish Group, chaired by the Data Protection Officer, is exploring the work required to improve the SAR situation across the Health Board which is expected to complete in Dec
- **Mandatory IG Training Compliance –** Training compliance reported to Mar 2021 IGG stands at 79%. There is a requirement for compliance to be at 95% and work continues to further improve staff completion of the mandatory training.
- **IG Breaches –** 1 breach (related to a SAR redaction error) has been reported to the ICO since the last IGG in September 2020. Financial compensation is being sought by up to 7 data subjects whose information was breached. To date, 26 breach reports to the ICO have been closed and their recommendations taken forward via the IG Partnership Group (IGPG). Between 1st September – 28th February 2021, 292 IG related incidents and near misses were confirmed on Datix. This number evidences robust identification and reporting of all levels of IG incidents, and is in line with the size of the Organisation. There have also been 6 complaints made to the ICO since July 2020, all focused on SARs and/or other data subjects' rights – these are not formally closed by the ICO and work continues to investigate and resolve all complaints.
- **IGG Lead Updates –** IGG receives update reports from all SDGs and Corporate Departments. An internal audit recommendation required that IGG and Audit Committee were made aware of any areas that had not submitted an update report. W&OD again did not submit a report.

Delegated action by the committee:

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

Main sources of information received:

- IG Update Report
- IG Key Performance Indicators
- Cybersecurity Report

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	23 June 2021