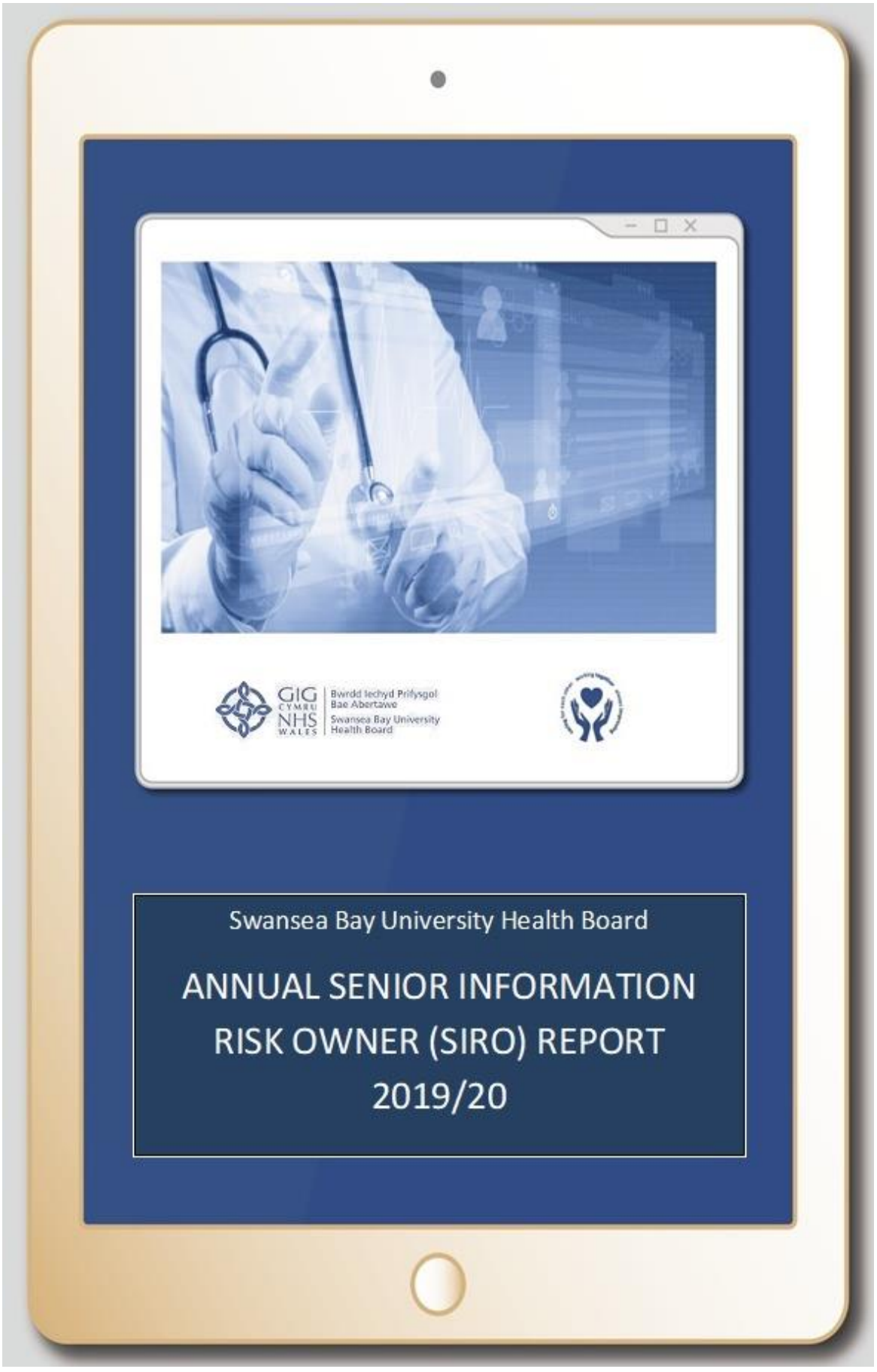

GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol Bae Abertawe
Swansea Bay University Health Board
Swansea Bay University Health Board
ANNUAL SENIOR INFORMATION RISK OWNER (SIRO) REPORT 2019/20

INTRODUCTION BY THE SENIOR INFORMATION RISK OWNER (SIRO)

It is a great pleasure to present the fourth annual report from the Senior Information Risk Owner (SIRO) from Swansea Bay University Health Board (SBU). The role of SIRO is responsible for advising the Board and the Accountable Officer about Information Risk and takes ownership of the organisation's information risk processes. The SIRO must advocate at the Board the reduction of information risk by ensuring effective use of resource, commitment and execution, along with appropriate communication to all staff. The aim is to create a culture in which information is valued as an asset and information risk is managed in a realistic and effective manner within the legislative frameworks that pertain to the Health Board.

There is a requirement for robust governance in order to remain legally compliant whilst also achieving an agility to ensure operational effectiveness so that progress is not undermined or damaged by poor Information Governance (IG) practices. To achieve this there is a comprehensive and complex range of national guidance and legislation with which SBU must comply:

- General Data Protection Regulation (2016)
- Data Protection Act (2018)
- Public Records Act (1958)
- Access to Health Records Act (1990)
- Freedom of Information Act (2000)
- Computer Misuse Act (2000)
- Environmental Information Regulations (2004)
- Caldicott Principles into Practice (C-PiP)
- Common Law Duty of Confidentiality
- Wales Accord on the Sharing of Personal Information (WASPI)
- Data Quality Standards and WHC
- Information Security Assurance - ISO 27001:2005 & 2013 Information security management (formerly BS7799)
- Networks and Information Systems (NIS) Directive
- Records Management, NHS Code of Practice
- Other appropriate legislation

During 2019-2020 the governance models and structures for the management of IG in SBU have further matured. There is good evidence that robust IG practices have been embedded across the organisation.

Recognising the breadth of the legislation, the SIRO Report is divided into five sections. Each section of the SIRO Report considers the progress and achievements in 2019-2020 and sets out the priorities and plans for 2020-2021; a summary is provided below.

The key achievements within the 2019-2020 SIRO Report can be summarised as follows;

Section 1, Information Governance provides comprehensive evidence of the work programme undertaken to ensure the organisation is compliant and demonstrating ongoing improvement and achievement against the requirements of data protection legislation, Information Commissioner's Office (ICO) guidance, national direction and local requirement. This section demonstrates action and improved assurance and compliance across all areas. Examples of IG achievements include:

- A very good Caldicott Principles into Practice (C-PiP) self-assessment score of 94.3%;
- Improved training compliance, at the end of 2019-2020 the Health Board stood at 87% overall compliance, a 2% increase from 12 months previously;
- Production of a new IG mandatory training video enabling staff, students, volunteers and temporary staff to access training in an accessible format at a time of their choosing;
- Implementation of the Information Asset Register (IAR). As of 31st March 2020 the IAR held details of 1816 assets, all quality assured;
- Achievement of 99.91% compliance with Subject Access Requests;
- 28 IG audits were conducted and a full analysis is available in the report demonstrating action plans and improvements;
- 37 Data sharing agreements supported and approved;

- A new process and template devised for Data Protection Impact Assessments, with 161 being supported and 30 approved;

- Robust IG support for new ways of working in response to the Covid-19 situation; and

- 501 Freedom of Information Act requests processed.

Section 2, Clinical Coding and Health Records provides evidence of the sustained transformation of the Clinical Coding Service following investment in 2016 and the ongoing work to continuously improve the Service and coding more activity electronically. The Health Board has achieved the Year End Coding Completeness Target for 2019-2020, attaining 99% coding completeness for the year end. Quality has also remained high during the period externally validated from the CHKS Benchmarking System. Depth of coding was on average 4.7 during 2019-2020, which was consistent with the previous year.

The Health Records section describes the significant investment in the Health Records Service, to modernise the management of the library services with the introduction of Radio Frequency Identification (RFID) technology to track records and change the way the service is delivered and deliver operational and organisational benefits. The section also demonstrates the ongoing challenges that the Service continues to face with retaining thousands of additional records that would have previously been destroyed in line with the embargo that is now in place across all Health Boards in Wales as a result of the Infected Blood Inquiry.

Section 3, Data Quality presents the SBU performance against the Data Quality standards for data submitted within the 2019-2020 financial year. SBU achieved 97.4**%**, and achieved 270 of the 277 checks in place; the Health Board are comparing extremely well alongside other Health Boards in Wales, as shown in the annual performance reports published by NWIS. Full details are detailed in the report along with other Data Quality and improvement initiatives.

Section 4, **Cyber Security** describes the increased attention and focus following the "Wannacry" Cyber Attack in May 2017, and the subsequent assessments and actions the Health Board has taken to improve security and reduce vulnerabilities. 2019-2020 has seen real progression with the resources given to tackle this serious threat including the establishment of a Cyber Security Team in Digital Services. Areas of improvement and change include:

- Establishing a Cyber Security Team, including appointment of a Cyber Security Manager and two Senior Cyber Security Specialists;

- The development of a new Cyber Security Policy to compliment the national and local policies;

- The development of a Cyber Security Impact Assessment document to compliment the Data Protection Impact Assessment and capture Cyber Security assessment of new procurements;

- Significant progress in identifying and replacing obsolete operating systems on desktop PCs and laptops;

- A full patching regime was implemented across all PCs, laptops and servers within the Health Board for all Microsoft software to reduce risk;

- Identification and removal of old, unnecessary, unsupported software installed across the estate;

- Adoption of a number of new Cyber tools from Welsh Government money, including Phishing simulation and training, Cisco Stealthwatch for network monitoring and new Cisco Firewalls;

- Adoption of National Cyber Security tools provided through NWIS, including a Security Incident and Event Monitoring solution and a Vulnerability Assessment Service; and

- Preparation and assessment for the implementation of the Network and Information Systems Directive (NIS-D).

SECTION 1 – INFORMATION GOVERNANCE

1.1 Accountability/Responsibilities and Governance Structures

The Information Governance Board (IGB) was established in 2016 and was renamed in May 2019 as the Information Governance Group (IGG). It is chaired by the Senior Information Risk Owner (SIRO) and oversees IG compliance, supports best practice and ensures that all Health Board information is:

- Confidential and secure;
- Of High quality;
- Relevant and timely; and
- Processed fairly.

IGG meets quarterly and provides reports to the Audit Committee. The IGG oversees the strategic direction of IG within the Health Board. In November 2018, a subgroup called the Information Governance Partnership Group (IGPG) was established. Its aim is to strengthen partnership working between the IG Department and IGG Leads, ensure consistency in IG approach across SBU, and to educate and support operational leads in areas of data protection legislation and good practice.

The IG Department delivers the operational Work Plan and continues to support the Health Board's drive for full compliance with data protection legislation and best practice.

1.2 Information Governance Strategy

During the period 2016-2017 SBU (ABMU at the time) approved its first IG Strategy. The Strategy covers the period 2017-2020 and includes the continuing development, implementation and embedding of a robust IG framework needed for the effective management and protection of the Health Board's information assets.

It outlines the Organisation's IG vision over this 3 year period. The Strategy underpins the Health Board's strategic goals and ensures that the information needed to support and deliver their implementation is available, accurate and understandable. The Strategy recognises that the legal framework underpinning IG in the UK changed in May 2018 with the introduction of the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. The Strategy prepared the Organisation for the new data protection legislation, and has continued to actively drive IG improvements across the Health Board during this period via completion of the Strategic Work Plan found in its appendices.

The following roles and responsibilities are clarified in the Strategy:

The Chief Executive

The Chief Executive is the Accountable Officer of the Health Board and has overall accountability and responsibility for IG. He/she is required to provide assurance, through the Annual Governance Statement, that all risks to the Organisation, including those relating to information, are effectively managed and mitigated.

The Senior Information Risk Owner (SIRO)

The SIRO is a Board Director with responsibility for advising the Accountable Officer and Board about Information risk. The SIRO has a key understanding of how the strategic goals of the Health Board may be impacted by information risk, across all types of information acquired, stored, shared and/or destroyed. They are the Board representative leading on IG. The SIRO provides an essential role in ensuring that identified information security risks are followed up and incidents managed. The Director of Corporate Governance was appointed as the SIRO on an interim basis in July 2018 and has subsequently been confirmed by the Board as the substantive SIRO in 2020.

The Caldicott Guardian

The Caldicott Guardian plays a vital role in ensuring that the Health Board satisfies the highest practical standards for handling patient identifiable information. Within the Health Board during the period 2019-2020, this role has been covered by the Director of Public Health and then the Interim Deputy Medical Director. Acting as the conscience of the Health Board, the Caldicott Guardian actively supports work to enable patient information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of patient information. The Caldicott Guardian also has a strategic role which involves representing and championing patient confidentiality and information sharing requirements and issues at senior management level. The Caldicott Guardian has responsibility for completing the annual Caldicott-Principles into Practice (C-PiP) self-assessment.

Information Governance Group (IGG) Leads

The nominated Leads that represent their Service Delivery Unit (SDU)/Corporate Department on the IGG are responsible in their unit for:

- Local IG Champion to promote and improve IG compliance and standards;
- Disseminating IG information;
- Signposting to and promoting of mandatory IG training;
- Signposting to appropriate IG and Information Security advice;
- Identifying Information Assets, their Owners and Administrators, supporting the mapping of information flows and production of data sharing agreements;
- Completing the IG Toolkit (or equivalent);

- Supporting auditing of IG and Cyber Security compliance;

- Identifying and recording IG risks, producing action plans to address these and reporting back to IGG on progress made;

- Supporting reporting and investigation of IG/Cyber Security breaches in their area, developing robust action plans and overseeing their completion, and reporting these back to IGG; and

- Nominating suitable representatives to sit on IGG Subgroups and Task and Finish groups.

Corporate Information Governance Function

The Corporate Information Governance Function resides within the Digital Services Directorate as part of the Director of Digital's portfolio. The Deputy Chief Digital Officer is the operational IG Lead for the Health Board and co-ordinates the IG priorities and strategic direction, reporting to the Chief Information Officer who also works closely with the SIRO. The Head of IG is responsible for overseeing the IG systems and processes within the Health Board and carrying out operational duties for the IG Lead. The Head of IG is the Data Protection Officer (DPO) and designated contact with the ICO. As part of this role they will ensure that the Health Board's annual Data Protection Registration is maintained and kept up to date. The IG Department provides expert advice, guidance and training on IG issues and delivers the IG Work Plan.

1.3 Compliance with Data Protection Legislation

The European Union General Data Protection Regulation 2016 (GDPR) informed the new UK Data Protection Act 2018 (DPA) which came into force in May 2018.

The Health Board uses a formal structure around the governance responsibilities for information. It has been proactive in ensuring that staff are aware of their responsibilities regarding the protection of staff and patients' information, and upholding citizens' information rights. It is necessary for the Health Board to provide assurance to the ICO at all times that compliance is continually reviewed and maintained at a high level going forward. Any gaps in compliance or areas that could benefit from further improvement form part of the IG Strategic Work Plan and are actioned at the earliest opportunity. Examples of actions completed during the period 2019-2020 are:

- Production and provision of an IG training video as an alternative to the e-learning IG training package – staff must complete their training by either method every two years to remain compliant with their mandatory IG training;

- Development of a number of guidance documents, including areas such as data subjects' rights, data sharing and the recording of meetings;

- Successful completion of the pilot all Wales NHS IG Toolkit to check the technical aspects of the process, with all outcome actions managed on a national basis;

- Revised templates and processes for completion of Data Protection Impact Assessments (DPIAs), including further embedding of these processes across the Health Board;

- Information flows analysed in light of Brexit;

- Progress made on the national IG Breach reporting process which is nearing completion; and

- Revised privacy notice templates and guidance.

1.4 Operational Work Plan and Key Performance Areas

In order to progress improvement, a Strategic Work Plan 2019-2021 was put into place thereafter. Detailed in the sections below are the key achievements in the period.

1.4.1 Information Asset Register (IAR)

One of the most important strands of work for the IG Department has been the ongoing establishment of a useful and robust Information Asset Register (IAR). This is vital in order to deliver on the IG strategy going forward and to comply with the Data Protection Act (2018).

The IAR is held on SharePoint which allows for detailed reporting as well as access by nominated Information Asset owners (IAOs) and Information Asset Administrators (IAAs) to actively manage and audit their information assets. As of 31st March 2020 the IAR held details of 1816 assets.

The IAR is a standing agenda item within the Information Governance Partnership Group (IGPG). The IG Department continues to offer guidance to IAOs & IAAs as necessary to assist IAOs/IAAs in managing their assets. A comprehensive guidance document is available to assist departments with their IAR completion.

1.4.2 Subject Access Compliance

Patient Subject Access Requests

The total number of patient Subject Access Requests (SARs) for the financial year 2019-2020 was 5985. This is an average of approximately 500 per month which is slightly higher than 2018-2019. The largest proportion of requests continues to be those received from solicitors. However, the Health Board has seen a slight reduction in the number of requests received during this period made by Government Agencies for patients' information.

The compliance rate for meeting the 28-day provision requirement for March 2020 was 99.91%, which maintains the high performance seen across the Health Board since the service was consolidated into a centralised department, which is based at the Neath Port Talbot Hospital (NPTH).

For the year 2019-2020 the centralised Subject Access Department will continue to operate from the NPTH site following boundary change with Cwm Taf Morgannwg University Health Board. It has been agreed that the SLA will be extended until March 2021 to facilitate the Princess of Wales (POW) element of all requests.

The requestors continue to benefit from the introduction and roll out of the secure information portal to share information safely and electronically; most solicitor requests and the majority of police requests utilise this.

	Requests Received	**No within target**	**No outside target**	**% within target**
Data Protection Act - 40 days				
2015-2016	4903	4898	5	99.9%
2016-2017	5501	5498	3	99.95%
2017-2018	5282	5279	3	99.90%
2018-2019	5770	5767	3	99.95%
2019-2020	5985	5980	3	99.91%
Government Agencies - 10 days				
2015-2016	925	925	0	100.00%
2016-2017	785	785	0	100.00%
2017-2018	1797	1797	0	100.00%
2018-2019	1939	1939	0	100.00%
2019-2020	1783	1783	0	100.00%

There is a procedure in place to check all records under the Subject Access process which ensures that all information contained in the records relate to the correct patient. Where information has been incorrectly filed there is a procedure in place to escalate these concerns to Governance leads and these are also recorded on Datix. These concerns are also included in the reports that are presented to IGG.

For the period 2019-2020, there were 149 reported incidents up until March 2020. This is consistent with the figure reported in 2018-2019.

Staff Subject Access Requests (SARs)

For 2019-2020 the Health Board processed a total of ten Subject Access Requests for staff. Staff SAR requests are managed through the Workforce and OD Directorate. As in previous years the breadth of information sought, particularly from email systems, is our greatest challenge. Measures to secure funding for the role that manages staff SAR have been put in place and should be enabled during the next financial year. A revised Staff SAR Policy has been developed and is aimed to be put into effect during 2020. Plans to have this in place earlier in 2020 have been affected by the Covid-19 outbreak.

1.4.3 Information Governance Training

The IGG has made IG training compliance a priority, setting a target of 95% overall compliance. Although this target has not yet been achieved, an improvement was made during the year. At the end of 2019-2020 the Health Board stood at 87% overall compliance, a 2% increase from 12 months previously.

Health Board IG training compliance is monitored on a monthly basis by the IG Department and quarterly by the IGG. IGG Leads are actively engaged via the receipt of the monthly reports and cascading this within their areas to enable the targeting of individual non-compliant staff or department that need improvement. Service Delivery Units (SDUs)/Corporate Departments are held to account at every IGG and actively supported by the IG Department to improve their IG training compliance.

Training is offered via completion of the Electronic Staff Record (ESR) based national e-learning package, or by staff watching the IG Training video and informing the IG Department of the three key words contained therin to evidence having watched it in full. The video is available in both English and Welsh, and can be accessed either on the Intranet or via YouTube.

Training is mandatory for all staff, to be completed when employment with SBU commences and refreshed every 2 years thereafter. Students, volunteers and temporary staff are directed to watch the video as they do not have ESR access.

1.4.4 National Intelligent Integrated Auditing Solution (NIIAS)

The National Intelligent Integrated Auditing Solution (NIIAS) is a software auditing tool used by all Health Boards/Trusts across NHS Wales. It is used to detect potentially inappropriate access to clinical records where employees may have accessed and/or viewed data they are not entitled to access. The purpose of the tool is to help the Organisation comply with its data protection responsibilities and to give the public the confidence in the Health Board's ability to ensure the confidentiality and privacy of their personal data.

NIIAS uses intelligent data triangulation and audit logs to detect when an employee may have misused their access rights. It then provides notifications to the IG Department for particular activity that may be of concern. Examples of this type of activity are as follows:

- Where an employee accesses their own SBU held electronic health record; and

- Where an employee accesses the SBU held electronic health record of a family member.

It is important to note that as this a national auditing tool, only the major national systems are covered. Local information systems are not covered by NIIAS. The national systems covered by NIIAS are as follows:

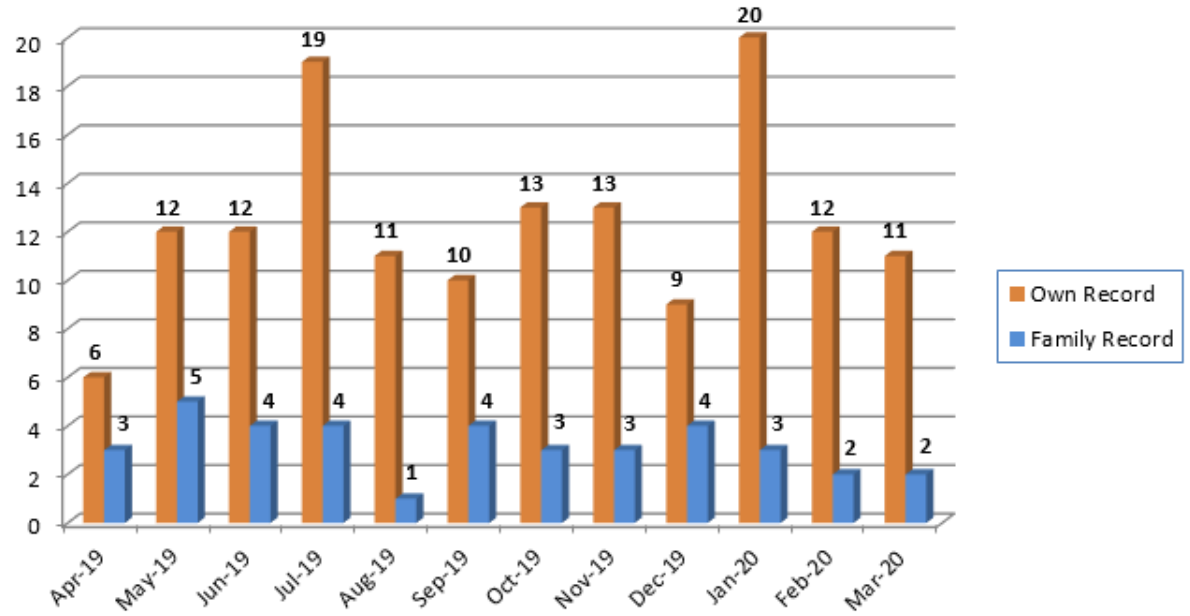
- Welsh Clinical Portal (WCP);

- AAA/Bowel Screening;
- Welsh PAS;
- CANISC (Cancer System);
- Electronic Staff Record (ESR);
- Welsh Demographic Service;
- Electronic master Patient Index (eMPI);
- Choose Pharmacy; and
- Welsh Emergency Department System (WEDS).

Further systems are to be brought into NIIAS coverage and the interface is currently under development:

- WLims (Pathology system); and
- Welsh Community Information Systems (WCCIS).

In addition, NIIAS triangulates with the National Active Directory (NAD) and ESR to validate identities of the user and employee when studying user activity. The total number of confirmed incidents for 2019-2020 are shown below, where incidents picked up by NIIAS were consequently confirmed as inappropriate access:



The level of confirmed incidents remains lower than that reported in many other Health Boards. NIIAS incidents are reported to the IGG and the low figures are achieved through IGG Lead support and intranet articles to raise awareness.

All incidents involving family records are escalated to the relevant line manager who investigates the incident under the Health Board Disciplinary Policy. IGG Leads are provided with a monthly breakdown of any outstanding/open incidents in their areas to ensure robust management of cases. NIIAS will continue to be a Key Performance Indicator (KPI) in 2020-2021.

1.5 IG Audits

A key component of a good IG model is the proactive improvement of practice and the mitigation of risk through the management of issues raised during IG Audits. In the period 2019-2020 SDUs and Corporate Departments have been subject to IG Department led Audits.

1.5.1 IG Audit Programme

The IG Audit Programme was planned for 2019 initially and the IGG received regular audit updates, from which IGG Leads were expected to ensure completion of action/improvement plans. As with the previous financial year, IGG Leads were asked to prioritise areas that would benefit from an IG Departmental Audit and any ICO reportable breach would trigger an IG audit of the relevant department.

Priority is given to conducting audits and any necessary follow up audits that relate to an ICO reported personal data breach, thereby providing assurance to the Health Board and the ICO that a proactive response is being taken in relation to incidents. Any audit reports where the audit was initiated due to an ICO reported breach may be made available to the ICO for evidence and assurance purposes.

IG Audit Programme prioritisation is detailed below:

1. Initial audits relating to an ICO reported incident;

2. Follow up audits relating to an ICO reported incident;

3. Follow up planned audits; and

4. Initial planned audits.

Any audits that go against the above prioritisation are brought to IGG for consideration unless a serious data protection risk is identified and an urgent audit is required which, in waiting for IGG consideration, would cause unnecessary and unbalanced delays.

IG Department Audits are rated and followed up as follows:

Audit rating	**Follow up timeframe**
Green = Satisfactory	No further follow up needed
Amber = Partial compliance	Further formal follow up required in 6 months
Amber = Partial compliance (if breach reported to ICO)	Further formal follow up required in 4 months
Red = No compliance	Further formal follow up required in 4 months
Red = No compliance (if	Further formal follow up required in 2 months

breach reported to ICO)	

Initial IG audits conducted during the financial year 2019-2020 are summarised as:

- 5 areas audited rated Green;
- 8 areas audited rated Amber; and
- 2 areas audited rated Red.

Follow up IG audits conducted during the financial year 2019-2020 are summarised as:

- 8 areas followed up rated Green;
- 4 areas followed up rated Amber; and
- 1 areas followed up rated Red.

The follow up on one of the areas originally rated Red, continued to rate as Red at follow up. Both red ratings were given due to concerns around the IG implications of the structural layout of the area audited. The original and follow up audits were used to support a business case to redesign and refurbish the area which is currently in progress. A further follow up IG audit will take place once the work has been completed.

Those follow ups that rated Amber had shown overall improvement, but due to their staff's mandatory training compliance not being above 95% the departments concerned were rated Amber and will be followed up at a later date to assess progress.

From each of the audits detailed improvement plans are developed and monitored.

1.6 Information Governance Incident Reporting

The IG Department provides reports at every IGG meeting on IG related incidents that have occurred within the Health Board. This provides oversight and assurance to the Group on the management of breaches and arrangements in place for areas of resource pressure or high risk. In addition, SDUs/Corporate Departments provide quarterly breach updates to the IGPG which support the sharing of learning, consistency of IG advice and promote good practice. IG breaches are managed in line with ICO guidance and the Health Board's IG Incident & Near Miss Procedure.

For the period 1st April 2019 to 31st March 2020, there have been 550 reported IG related incidents (this figure is approximate as figures can fluctuate slightly as incidents are reviewed, assessed and updated).

During the same period, 7 incidents were deemed to be of a severity requiring self-reporting to the ICO. These incidents are briefly summarised in the table below:

Date Reported	Reference	Breach Type
18/4/19	ICO_016	Disclosure – Paper
18/4/19	ICO_017	Disclosure – Verbal
25/4/19	ICO_018	Disclosure – Paper
23/5/19	ICO_019	Disclosure – Paper
13/7/19	ICO_020	Disclosure – Verbal
29/7/19	ICO_021	Lost/stolen paperwork (withdrawn*)
25/9/19	ICO_022	Lost/stolen paperwork

** This notification was later withdrawn as the missing paperwork was located.*

Each of these incidents has been investigated by the Health Board and the ICO, with appropriate remedial actions and improvements undertaken. These incidents have been formally closed by the ICO, with the exception of one incident which remains open while the ICO await the outcome of internal investigations and disciplinary proceedings. Recommendations received from the ICO are collated in a comprehensive action plan, the progress of which is monitored and reviewed by the IGPG and escalated to IGG if required. There has been no enforcement action taken by the ICO during the above reporting period.

A guidance document has been developed to support consistency across NHS Wales on the notification of data breaches to the ICO. The national working group has been co-led by SBU with input from the ICO. Consultations have been undertaken with IG professionals across NHS Wales and the ICO Breach Team, however completion of the document has temporarily been placed on hold due to Covid-19 priorities. A comprehensive review of the IG incident procedures and processes will take place upon publication of this document.

1.7 Health Board Information Governance Risk Log

Information Governance risks identified as being prevalent across the Health Board are recorded on the Health Board IG Risk Log. The management of these risks is undertaken locally by each of the areas affected with IG Department support, with entries transferred to local risk logs/registers. These risks are monitored at IGPG meetings.

There are 25 entries on the Health Board IG Risk Log. The risks have been reviewed and rescored, with the following results:

- Red (16+): 6
- Amber (10 – 15): 19

It should be noted that the scoring of each of the 25 risks is indicative only and may be subject to change when reassessed and incorporated into local Risk Registers. The risks noted indicatively as red are those prioritised and mitigated against by the Health Board. IG Risk will remain a standing agenda item at IGPG where individual risks on the Health Board IG Risk Log can be discussed at length, and included in IGG Lead updates/IGPG reports going forward.

1.8 Caldicott and Confidentiality

In 1997, the review of the uses of patient-identifiable information, chaired by Dame Fiona Caldicott, devised 6 principles for IG that could be used by all organisations with access to patient information. These principles are:

1. Justify the purpose(s) of using confidential information;

2. Only use it when absolutely necessary;

3. Use the minimum that is required;

4. Access should be on a strict need-to-know basis;

5. Everyone must understand his or her responsibilities; and

6. Understand and comply with the law.

During 2013 a further review of the Caldicott Principles and their relevance to the modern health and social care system was carried out and this was known as Caldicott 2. The recommendation from this was that a seventh principle be adopted:

7. The duty to share information can be as important as the duty to protect patient confidentiality: Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The Caldicott Foundation Manual: Principles into Practice sets out what organisations need to do and the arrangements that need to be in place to ensure patient information is handled appropriately and contains a C-PiP self-assessment that organisations are expected to complete annually. The Health Board has completed the online assessment for 2019-2020 and an accompanying Out Turn Report, scoring 94.3%, an increase from the 91% scored in 2018-2019:

	2018-2019	2019-2020
Overall %	91%	94%
Areas fully compliant	31	37
Areas partially compliant	9	3
Areas non-compliant	1	1

Areas requiring further action already form part of the IG Work Plan.

The Health Board has taken part in a pilot national IG Toolkit submission to enable the platform to be further developed, with the aim of it replacing CPiP.

1.9 Policy and Procedure Updates

During 2019-2020 the following policies and procedures that have IG content have been developed and/or reviewed, and then approved:

- NHS Wales Email Use Policy

The all Wales IG Policy and all Wales Information Security Policy are both currently under national review, with input given by SBU.

Policies, procedures and guidance documents will continue to be developed or updated during 2020-2021 to further support the IG agenda.

1.10 Information Sharing

SBU shares information with various other organisations in order to provide safe high quality healthcare for patients. These organisations include Welsh Government, Local Authorities, Voluntary Organisations and the Police. However, it is essential that patients can trust the Health Board and its partner organisations to share this information in a relevant, secure and confidential manner, thus protecting the patient's privacy at all times.

The Wales Accord on the Sharing of Personal Information (WASPI) has been endorsed by the Welsh Government as the 'single' information sharing framework for Wales. The purpose of the framework is to enable service-providing organisations directly concerned with the health, welfare, safeguarding, and protection of individuals and the public to share personal information between them in a lawful, safe and informed way. The framework consists of two elements: the Wales Accord on the Sharing of Personal Information and supporting local Information Sharing Protocols (ISPs). A range of guidance documents, templates and approved ISPs have been developed to assist partner organisations in implementing the framework.

Within the Health Board, the IG Department, with the support of the Caldicott Guardian, approve ISPs and other types of data sharing and processing agreements. A register of data sharing agreements is reported to IGG on a quarterly basis. During 2019-2020, 37 information sharing agreements were developed and approved.

1.11 Data Protection Impact Assessments (DPIAs)

One of the mandatory changes required under GDPR is that all new projects must undertake a DPIA. Article 35 of the GDPR states that DPIAs are mandatory for organisations when processing is likely to result in a high risk to the rights of the data subjects. DPIAs are fundamental to developing a privacy by design approach. The benefits of this approach include:

- Minimising privacy risks, building trust and having a robust risk management based approach to achieve effective information security and governance;

- Increasing awareness of privacy and data protection;

- Meeting legal obligations and less likely to breach data protection legislation; and

- Projects are less likely to be privacy intrusive or have a negative impact on individuals.

DPIAs are completed at the early stages of projects or proposed major new flows of information, and will then be reviewed throughout its lifecycle, or when a system change occurs. This allows SBU to find and fix problems early on, reducing the associated costs and damage to reputation that might otherwise accompany a breach of data protection legislation. The IG Department informs all staff about the need to complete a DPIA during mandatory IG training via its own ICO commended intranet pages and bulletins, as well as auditing compliance during delivery of the IG Audit Programme.

Robust DPIAs are developed with involvement from a range of stakeholders across the organisation that can contribute their knowledge and experience. The process is co-ordinated and supported by the IG Department, aligning the completion with existing risk and project management arrangements. The Department assures the DPIAs, bringing a log of all completed assessments to the IGG quarterly.

The DPIA screening questions have been embedded into the following departmental processes:

- Capital planning business cases;
- Informatics Directorate Project Review Group;
- Procurement;
- Investment Benefits Group; and
- Recovery & Sustainability for their Quality Impact Assessment.

March 2020 saw the initiation of the review to the DPIA process and templates in order to:

- Allow for clear implementation of the Cyber Security Impact Assessment (CSIA), which replaces the DPIA Part 2 form and separates cyber-security focused matters for IG forms;
- Allow for virtual support and completion to be undertaken as a matter of routine during Covid-19 adaptations;
- Allow for urgent proposals to be reviewed with reduced delays in order to support urgent implementation plans; and
- Acknowledge Covid-19 clinical needs in relation to the balance of IG risk.

Lessons learnt from Covid-19 DPIA support will guide future process and template updates.

A summary of DPIAs managed during the period of 2019-2020 are shown below:

Approved	30
In Progress	23
Rescinded (no longer required)	51
On hold (due to project reconsideration or Cyber Essentials Plus certification review)	15
Awaiting submission	40
Rejected (both due to Cyber Security concerns)	2

1.12 The IG Response to Covid-19

The Health Board's response to the Covid-19 pandemic requires a great deal of IG input. This includes:

- Ensuring IG representation at Digital Services Bronze and Health Board Covid-19 Gold Command Group meetings;

- Liaising with national IG programmes of work complementing the NHS in Wales' Covid-19 response to ensure a consistent and proactive IG approach across Wales, which included ICO attendance at all times;

- SBU IG leading on National IG Guidance Document regarding IG during Covid-19;

- Supporting national and local DPIAs and more concise IG reviews for new digital ways of working, including working from home and online patient consultations;

- Publishing Tier 3 Covid-19 specific privacy notices; and

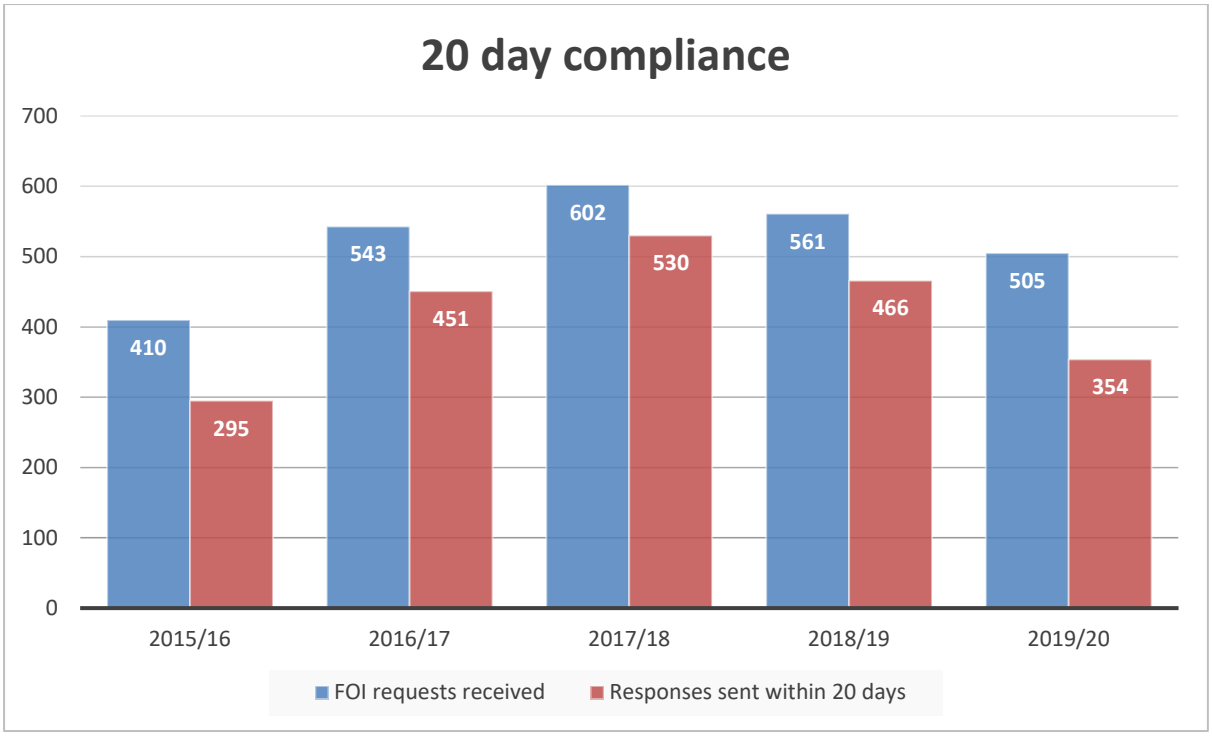
- Supporting Covid-19 specific national and local data sharing and processing agreements.

1.13 Freedom of Information Act (FOIA)

1.13.1 Summary

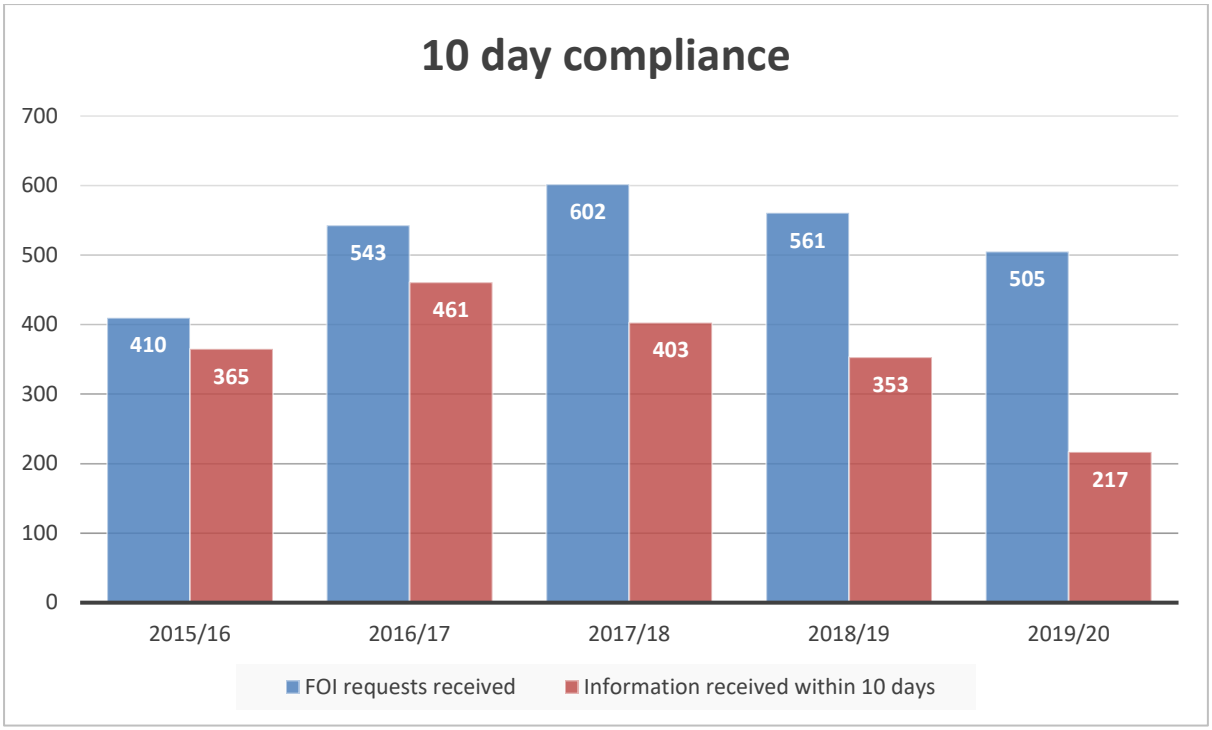
The Health Board received 501 FOIA requests in 2019-2020. The Health Board answered 70% of these requests on time (within the 20 working days). Appeals about the Health Board's responses remain low (1%).

The graph below illustrates the Health Board's performance since 2015-2016.



1.13.2 Performance

The FOIA team set a 10 working-day timescale to provide the required information so that the responses can be drafted, reviewed and appropriate exemptions applied if necessary. The changes to operational management arrangements have had an impact on the FOI process in that certain types of information may now need to be sourced from multiple delivery units rather than a single directorate, as was previously the case. However the ability to comply with the 10 day timescale can also be affected by the nature of the request as some can be complex often requiring numerous department's/directorate's involvement. Having seen a decline in compliance over the past year SBU are continuing to closely monitor this.



1.13.3 Potential for Monitoring by the ICO

The ICO currently monitors public authorities that repeatedly or seriously fail to respond to FOIA requests within the appropriate timescales. The Health Board has not been subject of any form of compliance monitoring by the ICO.

1.13.4 Internal Reviews

Any expression of dissatisfaction about the handling of an FOIA request is considered as a request for an internal review. An independent re-assessment of how the request was handled is conducted by someone who had no involvement with the original request. The Health Board received 6 complaints about its FOIA responses in 2019-2020. Of these all 6 requests were upheld. There have been no investigations from the ICO during 2019-2020.

Decision	Number
Upheld	6

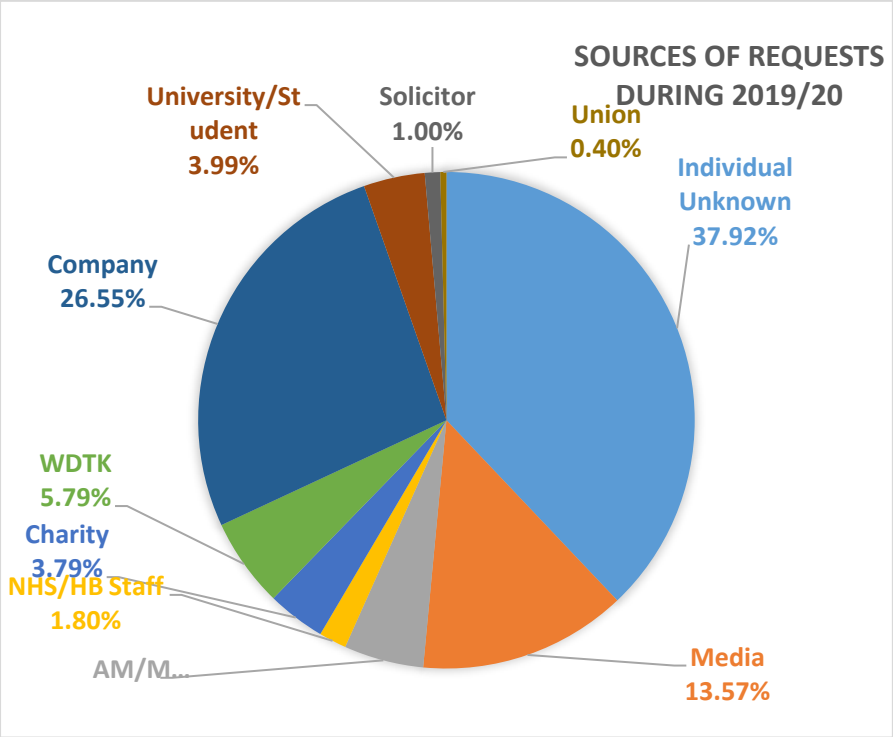
1.13.5 Request Trends and Subjects of Requests

The type of information being requested is diverse and the complexity of enquires varies. As in previous years, a significant number of requests focus on the efficiency, performance and transparency of the Health Board as an organisation (e.g. waiting lists, agency expenditure, cancelled operations, appointments, drug/pharmacy information etc.)

1.13.6 Source of Requests

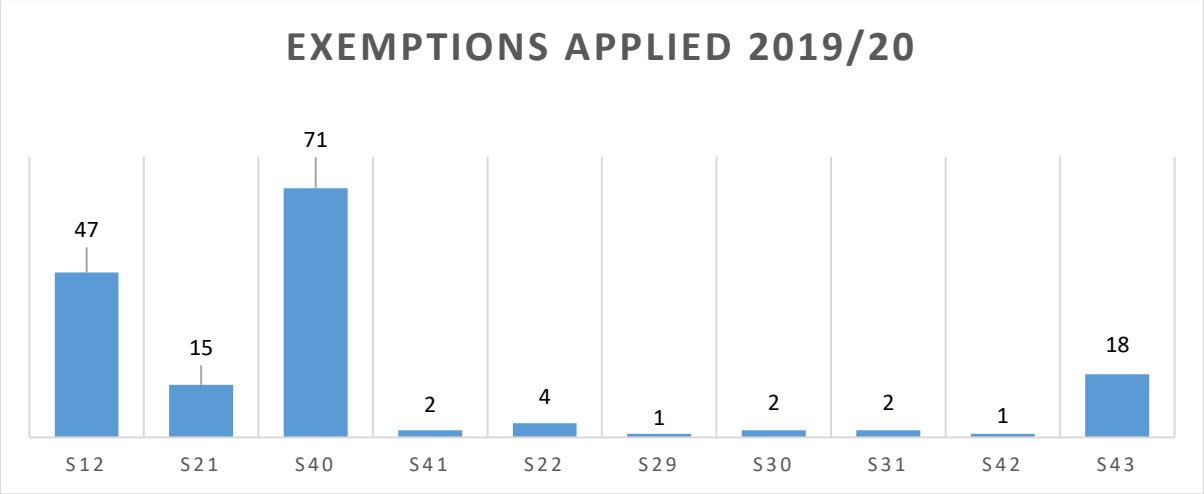
In accordance with FOIA, the Health Board maintains an 'applicant-blind' approach when providing information in response to requests. However, where that information is voluntarily provided by an applicant, the type of requester is recorded by the FOIA Team to help identify where the main demand for information originates.

37.92% of all requests to the Health Board were made by sources not identified. 5.79% of requests were made via the 'whatdotheyknow.com' – a website that allows requests to be submitted by members of the public via anonymous email addresses. Responses to these requests are automatically published online, further aiding the availability of FOIA disclosures.



1.13.7 Transparency

The FOIA carries an inherent presumption in favour of disclosure; information must be released unless one or more of the exemptions are engaged. Please find below the number and type of exemptions applied.



S12 - Cost of compliance exceeds appropriate limit
S21 - Information reasonably accessible to the applicant by other means
S22 - Information intended for future publication
S30 – Ongoing investigation or proceedings
S31 – Breaches IT security measures
S40 - Personal Information protected by the DPA/GDPR
S41 - Information provided in confidence (but only if this would constitute an actionable breach of confidence)
S42 - Legal professional privilege
S43 - Commercial interests

1.14 Looking Forward – Plans, Priorities and Challenges for 2020-2021

The IG agenda is wide and varied and therefore it is essential to have a planned and phased approach. The strategic actions for 2020-2022 have been noted on the IG Strategic Work Plan, prioritised according to risk assessment and knowledge acquired from breaches, audits and the IAR. It is a three year plan to ensure no required work is omitted whilst accepting that it will take this period of time to complete all actions with the available resources. This will ensure that SBU achieves and maintains full compliance with data protection legislation, whilst striving to improve and further embed its IG function, safeguarding all information it holds and supporting the delivery of the Digital Strategy.

Strategic work planned for the next financial year 2020-2021 includes:

- Production of further guidance documents regarding data subjects' rights;
- Review and development of CCTV and BodyCam Policy;
- Completion of the full IG Toolkit for the first time;
- Review and revise Tier 2 privacy notices;
- Finalise national IG Breach Scoring Guidance;

- Ongoing review of contracts and Data Processing Agreements; and
- Ensure the Health Board's approach to IG supports its Digital Strategy ambitions.

All progress will be monitored via formal reports taken to IGG and to Audit Committee quarterly.

SECTION 2 – CLINICAL CODING & HEALTH RECORDS

2.1 Clinical Coding Performance 2019-2020

Clinical coding information provides the key view of the clinical activity undertaken within a hospital setting, it is imperative that the coding activity carried out by the team is as complete as possible and as early as possible. Clinical coding information is used for a variety of purposes, to report on key quality and safety indicators such as condition specific mortality rates, and key efficiency and productivity indicators such as short stay surgery rates.

A timely view of these indicators is key to the effective monitoring and management of standards of performance, in addition, clinical coded data is essential to baseline and model service changes and support the organisation's commissioning processes. Welsh Government have acknowledged this requirement within the NHS Outcome & Delivery Framework and set out new challenging targets in April 2016 as outlined below: -

NHS Outcome & Delivery Targets require Health Boards to:

- Ensure that data completeness standards are adhered to within 30 days of discharge (instead of the previous 90 days);
- 95% on a monthly basis and 98% for any given rolling 12-month period; and
- Ensure both standards are applied across all episodes of admitted care at specialty, admission method level (elective and emergency) and all patient class (inpatient and day case) levels.

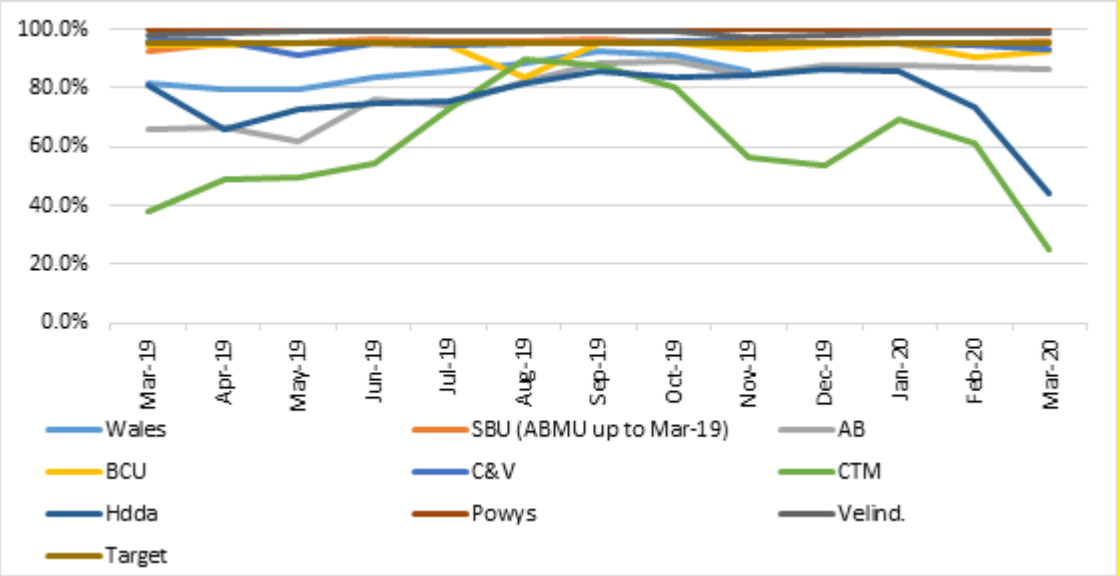
SBU has achieved the Coding Completeness Target for 2019-2020, attaining 99%. There were 1852 uncoded episodes as at 1st June 2020, out of a total of 155,777 episodes.

The data was submitted to NHS Wales Informatics Service (NWIS). Table 1 provides a breakdown of the 2019-2020 position as at 1st June 2020.

Table 1: Clinical Coding Completeness 2019-2020 - End of Year Position and End of Month Position

Position at Snapshot - end of month				End of Year		
Month	**Total No. of episodes**	**Total uncoded**	**Completeness %**	**Total No. of episodes**	**Total uncoded**	**Completeness %**
Apr-19	13197	523	96%	13220	151	99%
May-19	13652	582	96%	13668	123	99%
Jun-19	13286	378	97%	13309	128	99%
Jul-19	13978	533	96%	13993	122	99%
Aug-19	12780	475	96%	12789	122	99%
Sep-19	13039	493	96%	13055	161	99%
Oct-19	14024	617	96%	14074	169	99%
Nov-19	13202	965	93%	13249	149	99%
Dec-19	12228	602	95%	12255	144	99%
Jan-20	13177	576	96%	13178	147	99%
Feb-20	12185	628	95%	12208	182	99%
Mar-20	10764	698	94%	10779	254	98%
Totals	1555127	7070		**155777**	**1852**	

Table 2: All Wales Clinical Coding position – demonstrates SBU improvement and the sustained position in 2019-2020



Quality has also remained high during the period, the following depth and signs and symptoms of coding has been extracted from the CHKS Benchmarking System showing:

- Depth of coding was on average 4.7 during 2019-2020, which was consistent with the previous year; and

- Signs and Symptoms coding has decreased from 9.97% for 2018-2019 activity to 9.1% in 2019-2020 which in turn should result in more accurate quality information for reporting purposes.

The improvements and changes made in 2016-2017 have been sustained throughout 2019-2020, with continued training and development of the clinical coding trainee staff before the department was able to maximise the benefit of the additional resources.

In 2019-2020 the Clinical Coding Department benefited from an increase in productivity levels across the Service, due to clinical coding trainees becoming more proficient in their coding abilities and confidence levels. As more trainees become qualified Clinical Coders, this will decrease the assurance and support with queries that is required of the supervisory team and provide further opportunities to increase quality and productivity. The supervisory team continue to ensure that they focus on the quality of coded information through staff engagement, communication and service improvement initiatives. The service is enthusiastic and committed to achieving the challenging Welsh Government monthly targets of 95% compliance within 30 days of discharge and continues to build on all of the achievements made in recent years. Full plans and performance analysis are available in ***Appendix S2***.

To support the ongoing improvement of the service a comprehensive Audit programme is developed and undertaken throughout the year by the Clinical Coding Audit Lead. Full details are available in the Coding Performance information provided in ***Appendix S2***.

2.1.2 Clinical Coding Developments

Key developments during 2019-2020 that continue to improve the performance of the Clinical Coding Department have included:

- The Service Improvement Project and audit of single source documentation has led to an increased use of electronic information to code clinical activity. This has been possible by undertaking comparative audits on electronic source documentation and comparing it to the clinical documentation within the casenotes, to determine if there is sufficient quality information available;

- As a result of working with Clinical Leads, additional areas have also been identified for coding from electronic sources. Examples of these Services are the Renal day unit in Morriston where the Clinical Coding team have been working with clinical leads to improve the quality of the electronic information available for coding;

- Reports created to increase productivity of coding cancelled procedures and planned procedures;

- New Data Quality app developed to streamline reporting and data quality processes;

- New Missing Information app created to log all medical notes entering the coding departments without clinical information;

- The coding of current inpatient activity to increase performance levels even further;

- Coding of peripheral hospital activity at source;

- Development of eLearning coding modules with NWIS, to increase clinical coders' knowledge and skills;

- Participation of national user groups to improve quality of electronic information available for coding; and

- Development of a Clinical Coding awareness video for the Health Board Doctors' Induction Programme to improve quality of information documented by clinical staff, which was also presented to the Executive Board.

2.1.3 The Welsh Audit Office (WAO) Clinical Coding Follow Up Review 2018

The Clinical Coding Service have continued to implement and make significant progress against the outstanding actions and recommendations from the WAO Audit in 2018.

In February the Deputy Chief Digital Officer and the Clinical Coding Senior Management Team attended a Health Board Development Session where those present included the CEO, Chair, Executives and Independent Members, to present an overview on the progress and achievements that the Clinical Coding Service had continued to achieve over the past two years.

During the session an opportunity was also provided to show case the Clinical Coding storyboard that had been developed by the Clinical Coding Team for the Health Board Doctors' Induction Sessions. The storyboard highlights to all Clinical Staff the importance and essential requirement of documenting high standards of clinical information, within a patient "paper record" or on electronic systems, thus ensuring patients' activity is coded at the highest level.

2.2 Health Records

2.2.1 Health Records Modernisation

On the 8th November 2019, the SBU Health Records Service rolled out RFID Technology for the acute health record, across Singleton, Morriston and NPTH, with the objective of improving the clinical and logistical problems of a paper based health record, whilst modernising and improving the service, which the Health Records Service provided.

In readiness for “go live” considerable preparation work was undertaken between the Health Records Service and the supplier IDOX over an eighteen-month period to ensure the rollout was as seamless as possible.

Prior to the roll-out of RFID the Health Records Departments across the Service were full to capacity and in a position of not being able to store the number of records that were required to be stored. Filing bays that hold patients’ records were often over filled as there was no space available and due to this practice, on a number of occasions, sections of the libraries could not be accessed to retrieve records due to broken fixtures.

As a result of these practices and working conditions the role of a health records clerk was extremely physical. On an hourly basis staff would have to move patients’ records around the departments, in an attempt to create space to file patients’ records resulting in a duplication of tasks and effort for all staff, and on occasions transfer records between sites for filing purposes only. Also on a daily basis significant numbers of records would be stored on trolleys and in boxes due to no filing space being available.

Another significant pressure that the Health Records Service was under was the amount of time that Health Records Staff and the Supervisory Team spent looking for patients’ records and having to second guess on a daily/hourly basis, where the records could be. This situation resulted in a significant amount of duplication in terms of time and effort trying to locate the records. Prior to the roll-out of RFID this was an extremely resource intensive process that had to be followed, which also resulted in low morale and frustration within the teams across all Health Records sites.

This operational pressure also resulted in complaints being received by the Service due to records being unavailable and, on occasions, patients’ appointments/ procedures being cancelled due to the unavailability of the records.

The project was a significant undertaking for the Health Records Teams and the clinicians and administration staff across the organisation. There were initially some teething issues that caused some delay in the delivery of notes. However, “great things” then happened.

Benefits realised to date

There have been considerable benefits already realised across the service, which have included the RFID tagging of a patient’s record, Location Based Filing within the Health Records library areas, using barcode scanning technology and identification of a patient’s records location via fixed sensors. Thus enabling a patient’s records to be easily tracked on IFIT, located and made available as required and filed within any area of the Health Records Departments and reducing duplication of time and effort by health records staff in filing and locating patients’ records.

In addition to these benefits, for the first time the health records service has access to electronic KPIs that are automatically generated, through the new system (IFIT), which demonstrates the performance that the Service is providing on a daily basis, both within the Service itself, and to all stakeholders. This data allows the Service to

configure working teams more effectively based on demand and activity within the different functions of the Service.

Considerable operational benefits have already being realised within the Health Records Service, which includes the filing of a patient's records being much speedier, which has provided efficiencies to other areas of the Health Records Service. This has resulted in the Service at the end of each working day across all sites being in a position of having no notes left to file, no patients' records being stored on trolleys and boxes due to no space being available, and staff who would have previously being undertaking this function being able to undertake other roles within the health records service.

Health Records staff are also now able to pool their work by retrieving records from the location that the patients' records are tracked to irrelevant of the need/appointment reason for the patients' records and the Health Records Department's filing bays are no longer over filled with patients' records and locating them is much speedier.

Since the Service went live, the Health Records teams have tagged 276,000 records. In addition to these immediate benefits during the period prior to and since going live with RFID technology, the additional staff who were appointed as part of the Project have continued to accelerate the retention and destruction programme, which has continued to maximise the storage capacity that is available across all sites, by identifying patients records that would have previously been destroyed prior to the Infected Blood Inquiry, and moving these records to off- site storage areas which has created space on site for active patients records.

All of this has only been possible by rolling out RFID technology and has allowed the health records service to continue to be able to function in terms of storing active patients' records within the Health Records libraries, which would not have previously been possible.

The Health Records Service has also achieved significant efficiencies through the introduction of RFID by reducing the Health Records Establishment by 15WTE by the 31st March 2020.

As a result of Covid-19 in March 2020 there are further benefits that are anticipated to be made but have not been fully realised at this time. This is mainly due to the Health Records Service having to change its priorities and ways of working due to operational practices having to change as a result of significantly reduced Outpatient and Inpatient activity across the Health Board.

Further Benefits

- A 25% reduction of temporary files being created as a result of locating the original notes due to improved tracking and location based filing;

- A continuation in the reduction of the number of missing notes due to RFID technology and ability to locate notes on a timely basis; and

- To continue to maximise the storage capacity within each of the Health Records Libraries by location based filing.

2.2.2 Progressing the Digital Record

The further mitigation of the risks around the use of the paper health records are being managed through the delivery of digital transformation plans and implementation of the Digital Strategy. In this period the Health Board has established 5 Digital Transformation Programmes of work to deliver digital change. An essential Digital Enabling Programme has also been established to enable and support delivery. Each programme has the aim of enabling and supporting digitally enable care, health and wellbeing. There has been significant progress and success in each of the programmes during 2019-2020. Many of the programme plans were accelerated or amended in response to the needs of the organisation during the Covid-19 pandemic, increasing the scale and speed of digital transformation in SBUHB. Full digital plans are documented in Digital IMTP, and regular Digital Board update reports are presented to the Health Board.

Appendix S2 – Clinical Coding

Appendix S2 19-20 Final.docx

SECTION 3 – DATA QUALITY

4.1 The National Data Quality Performance Indicators

Good quality information is a fundamental requirement for the effective and prompt treatment of patients and to meet the needs of clinical governance, management information, accountability, health planning and service agreements. Poor quality data may not only affect a patient's treatment, but may also adversely affect income to the Health Board and the ability to accurately plan and develop the services needed by the community. Accuracy of information is also a key requirement and principle of Data Protection legislation.

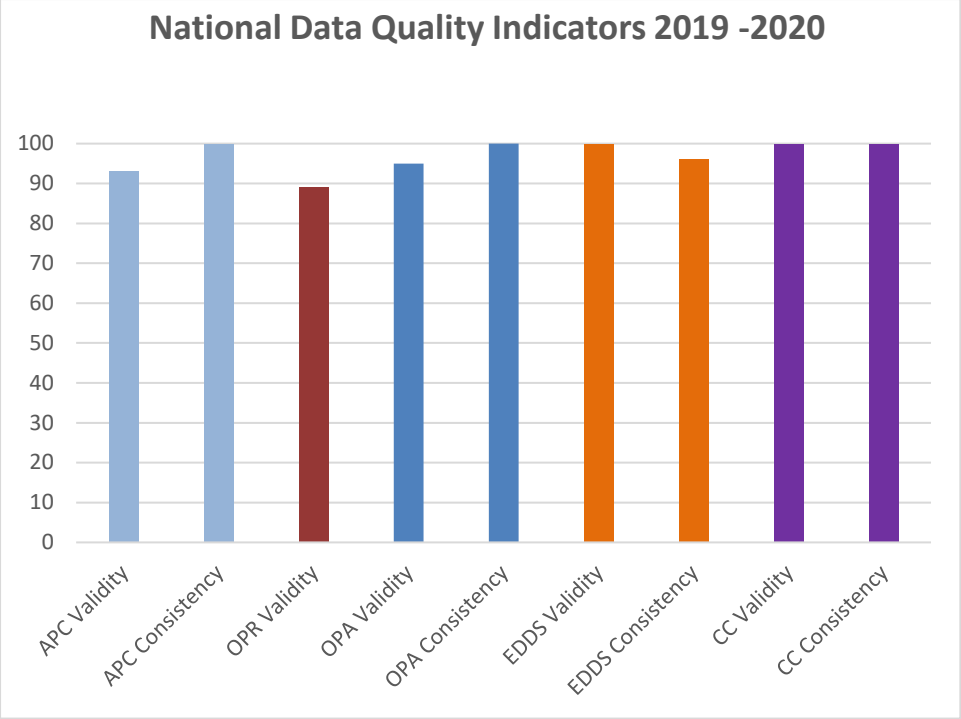
The Data Quality indicators are mandated within NHS Wales and cover the following datasets:

- Admitted Patient Care (APC) dataset;
- Outpatient Activity (OPA) dataset;
- Outpatient Referral (OPR) dataset;
- Emergency Department (ED) dataset; and
- Critical Care (CC) dataset.

The Data Quality Standards exist to ensure that nationally submitted data is monitored and improved so it can be used for both local and secondary uses. The indicators measure both the validity and consistency of the data and are assessed on a monthly basis as part of the data submission process. The validity indicators ensure that all data has the appropriate data item recorded for each record, whereas the consistency indicators measure related data items which are able to be compared to one another. For such related data items, the presence of a specific value in one field can restrict the value(s) that can be recorded in another. For example, where the primary diagnosis of a record is a maternity event, the gender attached to the record must be female.

SBU Health Board performance against these standards for data submitted within 2019-2020 financial year is 97.5%, achieving 270 of the 277 checks in place. SBU is comparing extremely well alongside other Health Boards in Wales, as shown in the annual performance reports published by NWIS (*available in* A*ppendix S4a*).

A summary of the work undertaken to achieve this performance of 97.5% and reasons why SBU did not achieve 100% performance for the Outpatient Activity (OPA), Outpatient Referrals (OPR), Admitted Patient Care (APC) and Emergency Department (ED) data sets is set out in *Appendix S4a.*



Section 4 – Detail of Data Quality performance - Appendix S4a

This performance was achieved by the Data Quality and Standards team actively monitoring all checks and addressing any issues where inaccuracies were seen to significantly rise or where targets were missed outside of our control.

4.2 Data Quality Improvement Work 2019-2020

The Data Quality Team has continued to support services and new developments and drive forward improvements during 2019-2020, despite having limited capacity. The work undertaken is essential to ensure that sound foundations are in place to sustain and improve the quality of data to support operational processes and service improvement.

Key achievements are listed below:

- Effective validation, monitoring and improvement of both local and national data checks;
- Supporting national system developments eg. WCP, WCCIS;
- Ensuring clinical systems are equipped to support service change and comply with national data requirements and standards;
- Provision of advice and guidance on how data should be recorded;
- Day to day support as and when data issues are identified and ensure plans are put in place for improvement;
- Implementation of national data set change notices;

- Representing SBU on national data/system groups;
- Feedback to users to emphasise the importance of accurate and timely data; and
- Daily adjustments on bed availability, ensuring occupancy is accurately reported both locally and nationally via the QS1 monthly submission.

Full details can be found in Appendix S4b.

4.3 Data Quality & Standards Improvement Plan 2020-2021

For the period 2020-2021 a detailed improvement plan has been developed that continues to prioritise the effective validation, monitoring and improvement of data quality in local and national systems.

There will be focused work on WPAS, WCCIS, InTouch outpatient system, National Data Quality Indicators, Non Admitted Activity, Virtual Activity, Transgender & Adoption Process and EMPI will be progressed to further improve processes and data quality assurances. Changes due to the Covid-19 pandemic will be a priority this year to ensure services can run smoothly and collect the data to support the changes.

The full description of the Data Quality Plan 2020-2021 is available in Appendix S4b.

Appendix S4 (a&b) – Data Quality

Appendix S4 19-20 Final.docx

SECTION 4 – CYBER SECURITY

5.1 *Key Achievements in 2019-2020*

Cyber Security refers to the body of technologies, processes and practices designed to protect networks, devices, programs and data from attack, damage or unauthorised access. The discipline is of increasing importance because the Health Board collects, processes, and store unprecedented amounts of data on computers and other devices. The majority of that data can be sensitive information, whether that be patient care information, financial data, personal information, or other types of data for which unauthorised access or exposure could have negative consequences. As the volume and sophistication of cyber attacks grow, NHS organisations that are tasked with safeguarding information need to take steps to protect sensitive business, patient and staff information.

The Covid-19 pandemic has seen the number of cyber attacks on the Health Board and its partners rise significantly, as a result of bad actors trying to exploit the pressures our staff and services face. This, along with the high profile 2017 Wannacry cyber attack, has raised awareness within the NHS and acts as a timely reminder that Cyber Security should be taken seriously and is essential for protecting services that increasingly rely on IT.

5.1.1 *Baseline Assessment – Stratia Report*

The Wannacry attack which affected NHS England was successful because it exploited a security weakness in the Windows operating systems. These systems had patches released by Microsoft in April 2017 but the affected organisations had not applied these patches in a timely manner.

In 2017 a baseline assessment was commissioned by Welsh Government to assess the cyber position across 12 organisations within NHS Wales in response to the Wannacry attack. A number of areas were identified where work was required to bring organisations up to the level of security required by UK standards, namely Cyber Essentials Plus, ISO27001/2, and the NIS-D. Following this initial assessment by the Stratia consultants, SBU commissioned Stratia in January 2019 to do a follow up vulnerability assessment using the same criteria as the initial assessment.

Below are the areas highlighted by the initial assessment, the work that has been undertaken over the year which was confirmed by the follow up assessment and the work still outstanding:

a) As part of the assessment it was highlighted that SBU were not up to date with applying Microsoft and other software security patches. This was common across NHS Wales. As a result, the actions undertaken in 2018-2019 included a full patching regime implemented across all PCs, laptops and servers within the Health Board for all Microsoft software. This was tested as part of the January 2019 vulnerability assessment and it confirmed that the regime implemented met all the required standards. A dashboard which shows the live

patching status for the computer servers (which hold the clinical and administration data) was developed as part of this process which is held up as good practice across NHS Wales. A Secure Managed Devices Working Group has been established to review and progress good practise established for Microsoft Security updates.

b) An area of risk identified was the use of third party software and it was clear that patching levels for this software was of increasing concern. Progress has been made on high volume third party applications. Third party software continues to be a challenge due to the number, variety and reliance of legacy systems on older versions of software. The ICT Department have an ongoing programme to categorise this software into 3 areas:

1. Software that is not needed (and removed):

2. Software that systems are reliant on certain versions and highlight these as legacy risks; and

3. Software with multiple versions, eg. Chrome, Adobe that can be standardised and updated accordingly.

To address these issues, the software will be ring fenced and limited to essential access only. This will limit the risk of this software not being on the latest versions and fully patched. A High Risk Software Review Working Group meets weekly to further this topic and reduce the risk of out of date and/or unnecessary software.

c) Another area identified within the audit was the presence of old, unnecessary, unsupported software installed across the SBU estate. To address this in 2018-2019, the Health Board appointed an ICT Asset Manager. This is an important role to ensure licence compliance and highlighting Cyber Security risks from running out of date software. The ICT Asset Manager is working through identifying software installed across the Health Board and will implement processes to agree and remove old, unnecessary and unsupported software, using the SNOW Asset Management System. The ICT Asset Manager is a member of the High Risk Software Review Working Group along with Cyber Security and Desktop Support staff who are progressing the identification and removal of old, unnecessary and unsupported software.

d) It was highlighted that network vulnerability scans should be undertaken at least once every 6 months. It was reported that a number of national products had been purchased to address this issue, namely NESSUS vulnerability scanner and the Security Incident and Event Management system (SIEM). NESSUS is a Vulnerability Management System which scans devices attached to the network for known security issues and report on the severity of them. This has recently been implemented at SBU and training for Cyber Security staff due in May 2020. Plans are in progress to commence vulnerability scanning.

SIEM has also been implemented which allows for centralised logging and alerting of suspicious events across all systems and networks. Local installation

has been implemented, with Health Board system cyber events feeding into the SIEM. Feeds from the Health Board Anti Virus and End Point Protection systems, the SBU Smoothwall Web Proxy (Internet Filter) and the local instance of the national Active Directory which collects information on failed login attempts, act as an early warning that there is a potential cyber attack by malware that is trying different passwords to login to a system. This provides a dashboard for security monitoring to ensure visibility of potential cyber threats and appropriate action taken by the Cyber Security team. Training for Cyber staff on operational use of the SIEM was scheduled for March 2020 but Covid-19 digital activities across NHS Wales means that this was postponed. The team, in conjunction with security resources in NWIS, monitor events on a daily basis. The training will ensure staff have the up to date knowledge to make the best use of the system in SBU.

e) The NIS-D requires further consideration and also data passing across local networks needs to be encrypted to protect against inappropriate access and possible interception. This is detailed as a priority for 2019-2020; work has been ongoing with NWIS to prepare and complete assessments and plans as detailed below.

5.1.2 Network and Information Systems Directive (NIS-D)

NIS-D was adopted by the European Parliament on 6 July 2016. The UK transposed the Directive into national laws on 9 May 2018 and identified Health as an Operator of Essential Services (OES).

WG is the competent authority under NIS-D and the role of this authority is to set thresholds against each of the security standards and to be the auditors of the legal standard. Health is awaiting further guidance from WG on how this will be implemented in Wales.

Progress in 2019-2020 includes the completion of the NIS-D Cyber Assessment Framework (CAF) with members of the national Operational Service Security Management Board (OSSMB). The National Cyber Security Centre (NCSC) has led on the development of the CAF which is a systematic method of assessing the extent to which an organisation is adequately managing Cyber Security risks in relation to the delivery of essential services.

5.1.3 Additional Cyber Security tools procured to enhance protection

In addition, the following Cyber Security systems are being implemented; these were funded by WG to enhance Cyber Security defences based on local needs:

System	Additional Protection
Network Monitoring and Visibility	Procured Cisco Stealth Watch (WG Cyber Security Funding) to allow real time monitoring and provide early warning for suspicious activity of the Health Board computer network, as well as retrospective analysis with the use of

	advanced machine learning. Early warning is critical in order to stop further potential damage caused by malicious attacks and limit the impact on availability/data loss.
Local Firewalls	Procured Cisco Firepower next generation firewalls (internal) to complement the Cisco Security Centre firewalls which protect the network traffic entering and leaving the Health Board. These provide additional internal security protection.

A Secure Networking Group has been established, as has a weekly review with the Network and Cyber Security Team to review network security. This Group provides expert knowledge in terms of the management of the newly procured solutions and effective proactive management of any network related security alerts from existing and new security tools.

5.1.4 Future Work and Compliance

The Cyber Essential Plus certification has recently been achieved by Local Authorities across Wales, and it is expected a similar approach will be taken by NHS Wales with WG. Compliance with this annually reviewed certification will largely align with NIS-D compliance, including annual independent vulnerability assessment as suggested by the Stratia report and now undertaken by SBU annually.

Cyber Security Policy

A Cyber Security Policy has recently been submitted to the IGG and approved for internal progression. This complements the All Wales IG and Information Security Policies. Cyber Security Strategy documents are also being developed to assist in directing the Health Board towards NIS-D compliance and to document functions of the Cyber Security Team.

Cyber Security Impact Assessment (CSIA)

Work has been undertaken with IG team members to develop a Cyber Security Impact Assessment document that will capture assurances during procurement process along with the DPIA documents.

5.1.5 Service Catalogue Development

The Service Catalogue provides a means by which IT services can be defined, configured, deployed and governed. The Service Catalogue is a highly effective resource in the event of an outage or Cyber Security attack, providing a complete up to date picture of the IT estate and supports decision making on priorities and risks. 505 services have been identified in the Service Catalogue.

5.1.6 Incident Management and Backup and Recovery

A Digital Services Incident Response and Business Continuity Plan has been developed and approved by the senior team. This document dovetails neatly with the organisation's Serious Incident Plan and the National Cyber Security Incident plan, and provides guidance on how to manage and communicate should an incident that affects digital services happen.

5.2 Development of strategy, capability, resources and operational priorities

5.2.1 Establishment of the Cyber Security Team

The growing threat posed by Cyber Security requires a coordinated and sophisticated approach. To achieve this, a Cyber Security department has been established as:

- Band 8a Cyber Security Manager;
- Existing Band 7 Cyber Security lead; and
- Additional two Band 6 posts as Cyber Security Specialists.

This has allowed for the setup of a Security Operations Centre to be established in a dedicated environment for the Cyber Team to monitor cyber events in real time and adopt a proactive approach to real time security alerting and taking appropriate mitigating actions and onward reporting. This is already providing benefits to the organisation in terms of identifying risks and providing rapid response to those risks.

The Cyber Security Team at SBU has strong partnership links in place. It works closely with a number of national groups as well as the Cyber Security Team at NWIS through OSSMB. The team also has membership of the NCSC's Cyber Information Sharing Partnership (CiSP) as well as the welsh WARP and Local Resilience Forum who have representatives from the Regional Organised Crime Cyber Unit TARIAN.

5.2.2 Enhanced Cyber Security Tools

A number of local tools and national systems have been in place for a number of years to protect against malicious attacks. The Cyber Security Team can now fully utilise these tools:

Local System	New Activity following formation of Cyber Security Team
Anti Virus and Endpoint Security – Kaspersky Endpoint Security renewed in 2020 which provides the Anti-Virus protection for desktop, laptop and server computers. In addition, Endpoint Security Management which forces encryption of USB memory sticks to protect data. Kaspersky are recognised as one of the Leaders in this field	Cyber Team have a dashboard displaying events and proactively manage this

Filtered Web Access – Web traffic from all devices on the Health Board network is sent via the Smoothwall Web Filter providing controls around which user groups can access which content types and provides additional protection to block access on known malicious sites	Rule sets are actively monitored and any sites highlighted as risks are actively blocked. This has been of particular importance during the Covid-19 pandemic to stop staff inadvertently accessing fake sites
Secure File Sharing Portal – This is used to securely transfer files to people outside of the organisation to protect against confidential information and/or personal data getting into the wrong hands	Cyber Team have improved the process to securely transfer confidential information and/or personal data. The process is much quicker than previously possible with a single resource and helps mitigate against work-around solutions which could inadvertently result in confidential information getting into the wrong hands
Secure Email – malicious emails coming into SBU through NHS Wales gateway are acted on efficiently and effectively	The newly established Cyber Security Team have developed a process to act upon malicious emails which have inadvertently come through the national email filter. These are daily events and without the new resources, would have taken substantially longer, especially when previously there was only one resource who could be training or in a meeting

5.2.3 Cyber Security Awareness

Rollout of a Cyber Security training module to raise awareness for staff; this is essential as staff are the biggest risk for any cyber security attack. A national Cyber Security Training Package has been deployed locally, through ESR elearning, which will offer a number of modules on improving awareness around Cyber Security.

Mandatory adoption of this training package is not in place yet. Until this is made mandatory and the training module has been completed by all staff, the Cyber Security risk associated with staff ill equipped to notice phishing or fraudulent emails remain at a high level. This has been taken to the mandatory training board but no agreement has been reached yet to adopt this essential training/awareness course.

In addition, a Phishing Simulation Campaign and Targeted Training software package has been procured from Welsh Government Cyber Security funding (Metaphish). This allows the Cyber Team to perform a simulated phishing attack and, depending on the staff response (clicks on a malicious link or not), provides a dashboard view on how many staff are aware of phishing emails and conversely who needs additional training to ensure they do not get exploited when real risk phishing emails come in. The training material complements the Cyber Security training module within ESR, but emphases the risk of phishing emails to raise awareness of Cyber Security risks and provide essential learning to mitigate against those risks.

5.2.4 Non-IT Managed Devices

Non-IT managed devices are devices such as medical equipment, building management systems, security cameras and point of sale tills, etc.. These still cause a significant challenge as they use software that may not be able to be patched or upgraded due to their FDA compliance for example. During 2020-2021 a control process will be rolled out for all new installations which will need to be completed prior to installation.

The use of the new Cisco Stealthwatch network monitoring solution will allow for the proactive detection and response to threats caused by non-IT managed devices.

5.2.5 Asset Management

The IT Asset Management Improvement plan is now in its third year. Planned key improvements for 2020-2021 include:

- A new Digital Asset Management Group has been established with members from Cyber Security and across ICT to assist the Asset Manager position with asset management;

- Improving the Starters and Leavers process;

- Software license harvesting process which will reduce unnecessary purchasing of software; and

- Integration of SNOW and Microsoft SCCM to allow for accurate software and hardware inventory.

5.2.3 Cyber Security Direction 2020-2021

Following on from the recent formation of the Cyber Security Team and procurement of new tools as detailed above, the immediate direction of the team is to establish itself and the use of the tools provided into the day to day workings of the Health Board to ensure the ongoing security and availability of digital services and systems.

The recent formation of the Security Operations Centre will enable a fast response to security events and incidents across the Health Board, but recent changes to working from home may require new ways of working in response to these new challenges.

The imminent enforcement of the NIS-D in NHS Wales will require meeting compliance and external auditing of the security controls and measures in place. To address this, a Cyber Security Strategy is being developed to address the scope of NIS-D compliance and ensure the Health Board is ready to meet the requirements of any external audits. The possible requirement to achieve Cyber Essentials Plus certification is also being considered as part of the objectives of this Strategy.

The rapid migration of services and systems to new solutions such as O365 and possibly Azure (The Cloud) has many security considerations, and potentially changes the threat landscape for the whole organisation. The Cyber Security Team will play an

integral part in the discussions and implementation both locally and nationally for any proposed changes, to protect the future confidentiality, integrity and availability of Health Board's systems and data.