Abertawe Bro Morgannwg University Health Board

ANNUAL SENIOR INFORMATION RISK OWNER (SIRO) REPORT 2018/19

INTRODUCTION BY THE SENIOR INFORMATION RISK OWNER

It is a great pleasure to present ABMU's third annual report from its Senior Information Risk Owner (SIRO). The role of SIRO was established in ABMU in 2016 and 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 and 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 compliant legally whilst also achieving an agility to ensure operational effectiveness so that progress is not undermined or damaged by poor Information Governance practices. To achieve this there is a comprehensive and complex range of national guidance and legislation with which ABMU must comply:

- General Data Protection Regulation (May 2018)
- 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 Legislation (2004)
- Caldicott Principles in Practice (CPIP)
- Common Law duty of confidentiality
- Wales Accord to Share Personal Information(WASPI)
- Data Quality Standards and WHC
- Information Security Assurance - ISO 27001:2005 & 2013 Information security management (formerly BS7799)
- Records Management, NHS Code of Practice
- Other appropriate legislation

During 2018/19 the governance models and structures for the management of Information Governance in ABMU have matured. There is good evidence that robust Information Governance practices have been embedded across the organisation.

Recognising the breadth of the legislation, the SIRO report is divided into four sections. Each section of the SIRO report considers the progress and achievements in 2018/19 and sets out the priorities and plans for 2019/20, as summary is provided below.

The key achievements of the 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 the General Data Protection Regulations (GDPR). A GDPR Work Plan was devised based around the Information Commissioner Office's 12 steps to GDPR compliance guidance. 51 actions were completed by the end of 2018, with 8 being added to the Strategic Work Plan for 2019-21. This demonstrates action and improved assurance and compliance across all areas.

Further examples of progress include

- A very good Caldicott in Practice self-assessment score of 90%.
- Improved training compliance, at the end of 2018/19 the Health Board stood at 85% overall compliance, a 25% increase from 12 months previously.
- Implementation of the Individual Asset Register (IAR). As of 31st March 2019 the IAR held details of 1834 assets, all quality assured.
- Achievement of 99.95% compliance with Subject Access Requests

External validation of the improvements have also been achieved during the period. Internal Audit audited the IG Framework within ABMU in 2016 where Limited Assurance was noted. A follow up audit was performed in November 2017 where significant improvements were noted and an overall rating of Reasonable Assurance was achieved. In November 2018, Internal Audit undertook their review of the GDPR Work Plan which resulted in their report noting an achievement of **Substantial Assurance attained.** In addition 41, IG audit were conducted by the team and a full analysis is available in the report demonstrating action plans and improvements.

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 in the department. The Health Board has achieved the Year End Coding Completeness Target for 2018/2019, **attaining 99%**

coding completeness for the year end. Quality has also remained high during the period validated by the national Benchmarking System, CHKS. Depth of coding was on average 4.7 during 2018/19, which was higher than the previous year of 4.6.

The Health Records section describes the significant investment in 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.

It also demonstrates significant progress towards digital records with key achievements including,

- Roll out of access to Patient records through the Patient Knows Best Platform
- Availability of All Wales diagnostic results and clinical documents via the Welsh Clinical Portal
- Increase in roll out of electronic referrals and Consultant electronic prioritisation
- Electronic Pathology Test Requesting implemented NPTH & Morriston inpatient wards
- Access to the summary GP record implemented across all sites
- SIGNAL, Electronic White Board Solution: creating efficiencies and safety improvements.
- Community Mobilisation, 100% of community staff (2400) now using an iPad to improve patient care and deliver efficiencies.
- Business Intelligence (BI) and Analytics. There has been investment in market leading BI & analytics tools -QlikView & QlikSense.

Section 3, Data Quality presents the ABMU Health Board performance against the Data Quality standards for data submitted within 2018/19 financial year. ABMU achieved 98**%**, achieving the required target for 272 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 increase attention and focus following the Cyber Attack in May 2017 Wannacry, and the subsequent assessments and actions the Health Board has taken to improve security and reduce vulnerabilities. 2018/19 have seen areas of improvement including

- Significant progress in identifying and replacing obsolete operating systems on desktop and laptops
- A full patching regime was implemented across all PC, 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
- A significant improvement was made by implementing the authentication of medical devices, and allowing only access to areas of the network the device requires.
- Preparation and assessment for the implementation of Network and Information Systems Directive (NISD)

SECTION 1 – INFORMATION GOVERNANCE

2.1 Accountability / Responsibilities and Governance Structures

The Information Governance Board (IGB) was established in 2016, chaired by The Senior Information Risk Owner (SIRO) to oversee IG compliance, support best practice and ensure that all Health Board information is:

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

IGB meets bi-monthly and reports to the Senior Leadership Team and to the Audit Committee for assurance. The IGB 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 IGB Leads, ensure consistency in IG approach across ABMU, 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 good practice.

2.2 Information Governance Strategy

During the period 2016/17 ABMU approved its first IG Strategy. The Strategy covers the period 2017-2020 and includes the continuing development, implementation and embedding of a robust Information Governance 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 has prepared the Organisation for the new data protection legislation, and will continue 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 should be an Executive 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 member leading on IG. The SIRO provides an essential role in ensuring that identified information security risks are followed up and incidents managed. The Executive Medical Director & Chief Information officer became the Board's first SIRO in July 2017, superseded by the Director of Corporate Governance / Board Secretary in July 2018. The Board Secretary became the Deputy SIRO, superseded by the Associate Director of Informatics in July 2018.

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, the Director of Public Health is the nominated Caldicott Guardian. 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 (CPiP) self-assessment.

Information Governance Board (IGB) Leads

The nominated Leads that represent their Service Delivery Unit (SDU) / Corporate Department on the IGB 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 Information Security compliance;
- Identifying and recording IG risks, producing action plans to address these and reporting back to IGB on progress made;
- Supporting reporting and investigation of IG/Security breaches in their area, developing robust action plans and overseeing their completion, and reporting these back to IGB; and

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

Corporate Information Governance Function

The Head of Digital Records and Information Assurance is the operational IG Lead for the Health Board and co-ordinates the IG priorities and strategic direction, reporting to the Associate Director of Informatics 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 Information Commissioner's Office (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 Plans.

2.3 GDPR

During the period 2017/18, UK and European Union Data Protection laws were based on a 1995 European Union (EU) Directive 95/46/EC; in the UK this was seen as the Data Protection Act 1998. The European Union GDPR was the EU's way of harmonising the different laws across the EU into a single regulation applicable across all EU member states, implemented in May 2018. It built on previous privacy and data protection legislation but aimed to provide more protection for consumers (ABMU's patients) and more privacy consideration for organisations (the Health Board). There are some clear content differences between the GDPR and the DPA 1998 whilst maintaining the basic concepts of providing a duty of confidence and expectations of that confidence by the citizen. The GDPR informed the new DPA 2018 which also came into force in May 2018.

The improvement work and developments in IG over the past few years on the way in which ABMU manages, uses and stores information in some instances provided a solid foundation for the demands of the new data protection legislation. ABMU already had sound and strong professional practices, which have been reviewed and further built upon to ensure ongoing compliance with the new legislation.

The GDPR applies to organisations offering goods and services (i.e. health care through the NHS) or monitoring the behaviour of citizens regardless of wherever the organisation is based and as long as the organisation is processing an EU citizen's data. This takes into account the increasing complexities of the collection and use of digital data – which was not included in the DPA 1998.

The Health Board uses a formal and informal 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 for many years irrespective of the new regulation, however it was recognised that much more needed to be done in this area.

A GDPR Work Plan was therefore devised, and progress against this was reported to IGB as well as nationally. This was based around the ICO's 12 steps to GDPR compliance guidance. 59 individual tasks were noted on the ABMU GDPR Work Plan,

and the timescales were realistically set to allow for 50 of them to be completed by the end of 2018. In practice, 51 were completed in this timeframe, and the remaining 8 have been added to the Strategic Work Plan for 2019-21.

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.

2.4 Operational Work Plan and Key Performance Areas

In order to progress improvement, the specific GDPR Work Plan was followed until December 2018, and a revised Strategic Work Plan 2019-21 put into place thereafter. Detailed in the sections below are the key achievements in the period.

2.4.1 Information Asset Register (IAR)

The internal Audit Review in January 2016 and the ICO Audit September 2016 identified the need for the development of the Information Asset Register (IAR). An information asset is defined as:

> *'An identifiable asset owned or contracted by an organisation which is of value to the business. It will include databases, applications, technical computing infrastructure, paper record stores, and policy/process/ educational related materials'.*

One of the most important strands of work for this financial year has been the ongoing establishment of a useful and robust IAR. This is vital in order to deliver on the IG strategy going forward and to comply with the new data protection legislation.

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. Development work and final testing of the IAR was completed by March 2019. As of 31st March 2019 the IAR held details of 1834 assets, all quality assured.

The IAR User Group that was established to offer help and support to IGB Leads, IAOs and IAAs was incorporated into the IGPG from November 2018 and is now a standing agenda item in that forum.

2.4.2 Subject Access Compliance

Patient Subject Access Requests

The total number of patient Subject Access Requests (SARs) for the financial year 2018-2019 was 5770. This is an average of approximately 481 per month which is slightly higher than 2017/2018. The largest proportion of requests continues to be those received from solicitors. However, the department continues to see a considerable increase in the number of requests received during this period made by Government Agencies for patients' information.

In line with the new GDPR regulation from 25th May 2018, the department has implemented a new way of working to ensure compliance with the new provision timescale of 28 days; patients who request their information electronically can now receive the information in this format. No fee is charged for this process in line with the GDPR regulations which has resulted in a loss of approximately £170,000 per annum.

The compliance rate of meeting the 28 day provision requirement at March 2019 was **99.95%,** which maintains the high performance seen across the Health Board since the service was consolidated into a centralised department, based at the Princess of Wales Hospital. The department continues to benefit from the introduction and roll out of the secure information portal to share information safely and electronically with requestors; 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				
15/16	4903	4898	5	99.9%
16/17	5501	5498	3	99.95%
17/18	5282	5279	3	99.90%
18/19	5770	5767	3	99.95%
Government Agencies - 10 days				
15/16	925	925	0	100.00%
16/17	785	785	0	100.00%
17/18	1797	1797	0	100.00%
18/19	1939	1939	0	100.00%

The department follows a process to check all records released from the Subject Access Department to ensure information contained in the records relate to the correct patient. Where information has been incorrectly filed whilst in use across the Health Board, incident reports are logged on the Health Board's incident management and reporting system, Datix, and these are escalated to governance leads. These figures have continued to be reported to IGB from July 2016, and for 2018/2019 there were 148 reported incidents up until March 2019 which is a considerable increase from 2017/18. This is more likely to be an increase of reporting of incidents rather than an increase of incidents themselves.

For the year 2019/20 the centralised Subject Access Department will transfer across to the NPTH site following boundary change with CTHB. The department will continue to facilitate the POW element of all requests under an agreed SLA for 12 months from the 1st April 2019.

Staff Subject Access Requests

For 2018/19 the Health Board processed a total of 9 Subject Access Requests (SAR) for staff. Staff SAR requests are managed through the Workforce and OD Directorate by a nominated individual who at times has support from other workforce staff. As in previous years the breadth of information sought, particularly from email systems, is

our greatest challenge. A revised Staff SAR Policy is being developed and is aimed to be in place by the end of 2019.

2.4.3 Information Governance Training

The IGB has made IG training compliance a priority, setting a target of 95% overall compliance. Although this target has not been achieved, significant improvement was made during the year. At the end of 2018/19 the Health Board stood at 85% overall compliance, a 25% increase from 12 months previously.

Health Board IG training compliance is monitored on a monthly basis by the IG Department and bimonthly by the IGB. IGB 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. SDUs / Corporate Departments are held to account at every IGB and actively supported by the IG Department to improve their IG training compliance.

Training is offered via face to face open access sessions, in house departmental sessions or via completion of the Electronic Staff Record (ESR) based national e-learning package. Training is mandatory for all staff, to be completed when employment with ABMU commences and refreshed every 2 years thereafter. Separate arrangements have been made for students, volunteers and temporary staff.

2.4.4 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 care record;
- Where an employee accesses the 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:

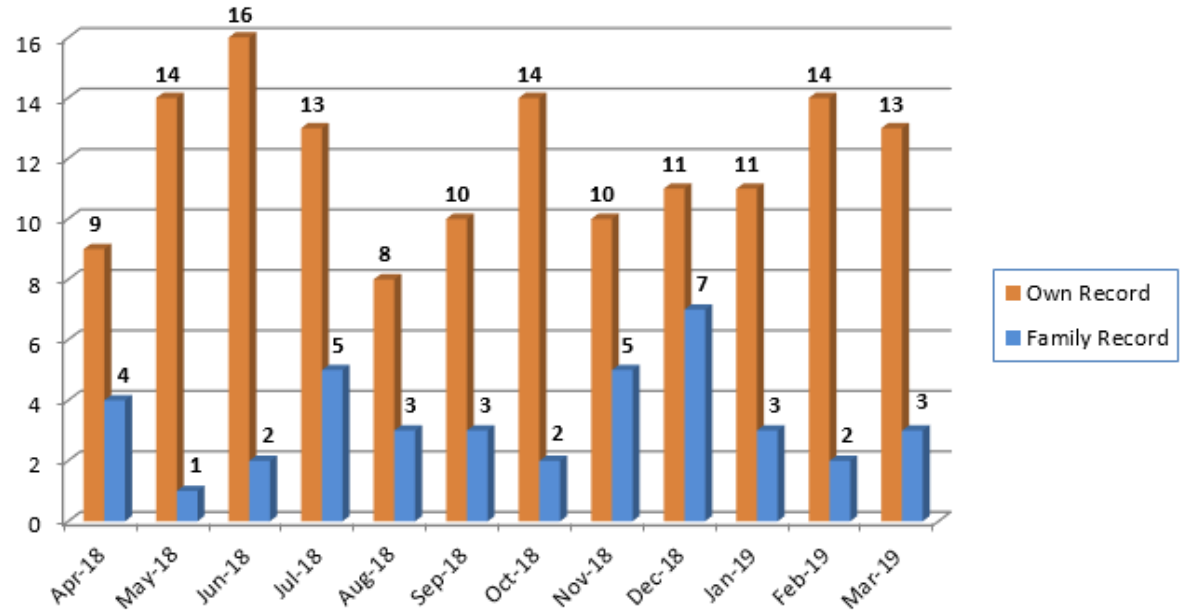
- Welsh Clinical Portal (WCP)
- AAA / Bowel Screening
- Welsh Patient Administration System (WPAS)
- CANISC Cancer System
- Electronic Staff Record (ESR)
- Welsh Demographic Service (WDS)

- Electronic Master Patient Index (EMPI)
- Choose Pharmacy
- Welsh Emergency Department System (WEDS)

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

- Laboratory Information System (LIMS)
- 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 2018/19 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 IGB bimonthly and the low figures are achieved through IGB Lead support, intranet articles to raise awareness and coverage during IG face to face mandatory training.

All incidents involving family records are escalated to the relevant line manager who investigates the incident under the Health Board Disciplinary Policy. IGB 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 2019/20.

2.5. 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. ABMU has been subject to three main types of audit:

1. Wales Audit Office follow up Audit;

2. Internal Audit follow up Audit; and
3. IG Department led Audits.

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

2.5.1 Wales Audit Office (WAO) follow up Audit

The WAO audited the IG Department as part of a wider IT Infrastructure follow up Audit in August 2018. The resultant report has not yet been received by ABMU but will be reviewed and an action plan put together on receipt.

2.5.2 Internal Audit follow up Audit

Internal Audit audited the IG Framework within ABMU in 2016 where Limited Assurance was noted. A follow up audit was performed in November 2017 where significant improvements were noted and an overall rating of Reasonable Assurance was achieved.

In November 2018, Internal Audit undertook their review of the GDPR Work Plan which resulted in their report noting an achievement of Substantial Assurance attained. There was only one recommendation, which related to the submission of IGB Lead update reports to the IGB, and this was actioned immediately.

2.5.3 IG Audit Programme

The IG Audit Programme was planned for 2018 initially and the IGB received regular audit updates, from which IGB leads were expected to ensure completion of action / improvement plans. As with the previous financial year, IGB Leads were asked to help 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
4. Initial planned audits

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

Between April 2018 and June 2018, the IG Department Audits were rated and followed up as follows:

Overall Grading:
Green = satisfactory (needs no further follow up) Amber = partial compliance (requiring formal follow up in 6 months) Red: = non-compliant (requires formal follow up in 4 months)

From July 2018, the IG Department Audits were 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 breach reported to ICO)	Further formal follow up required in 2 months

Initial IG audits conducted during the financial year 2018/19 are summarised as:

- 3 areas audited rated Green
- 33 areas audited rated Amber
- 5 areas audited rated Red

Follow-up IG audits conducted during the financial year 2018/19 are summarised as:

- 5 areas followed up rated Green
- 4 areas followed up rated Amber
- 4 areas followed up rated Red

Those follow ups that rated Amber had shown considerable 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.

2.6 Information Governance Incident Reporting

The IGB receives bimonthly updates from both the IG Department and the SDUs / Corporate Departments (via IGPG post November 2018) on IG related incidents that have occurred within the Health Board. This allows oversight and breach management as well as identification of risk factors across the Health Board and the sharing of learning across differing areas with similar issues. IG breaches are managed in line with the IG Incident and Near Miss Procedure.

From the introduction of the General Data Protection Regulation on the 25th May 2018 to 31st March 2019, there have been approximately 660 reported IG related incidents (this figure is approximate as figures may fluctuate as incidents are reviewed, assessed and updated).

During the 2018/19 financial year period, 15 incidents were deemed to be of a severity level requiring self-reporting to the ICO. These 15 incidents are briefly summarised in the table below:

Date Reported	Ref	Breach Type
01/06/18	ICO_001	Disclosure – Paper
22/06/18	ICO_002	Lost / stolen paperwork
29/06/18	ICO_003	Unauthorised Access
17/08/18	ICO_004	Disclosure - Verbal
25/08/18	ICO_005	Disclosure - paper
25/08/18	ICO_006	Disclosure – electronic
05/09/18	ICO_007	Disclosure – electronic
24/09/18	ICO_008	Disclosure - paper
26/09/18	ICO_009	Lost / stolen paperwork
12/10/18	ICO_010	Disclosure - paper
10/12/18	ICO_011	Disclosure – paper
31/12/18	ICO_012	Disclosure - electronic
11/01/19	ICO_013	Unauthorised Access
19/01/19	ICO_014	Disclosure - paper
08/03/19	ICO_015	Disclosure – verbal

Each of these incidents has been fully investigated by the Health Board and the ICO, with appropriate remedial actions and improvements undertaken. The majority of these incidents have since been formally closed by the ICO, however a small number remain open while the ICO await the outcome of on-going 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. There has been no enforcement action taken by the ICO during the above reporting period.

The process for reporting breaches to the ICO is currently being considered by a national working group, co-led by ABMU and with ICO input, to support consistency of scoring and reporting across NHS Wales. The Health Board processes and procedures will be reviewed and updated upon completion of this guidance document.

2.7 Information Governance Risk Register

The Health Board IG Risk Register is managed by the IGB. The IAR and IG audits are used to identify and assess risk, and the Strategic Work Plan reviewed accordingly with the aim of mitigating risks.

The risk register has identified 20 risks that score between 9-20. The themes on the Risk Register included:

- Lower than optimal mandatory training compliance;
- Information sharing and release to third party;
- Asset management and register;
- Breach and Incident Mangement;
- Readiness and adherence to GDPR;
- Staff Subject Access process;
- Poor practice and co-odination of release of information to the Police; and
- Implementation of Data Protection Impact Assessments.

2.8 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 CPIP self-assessment that organisations are expected to complete annually. The Health Board has completed the online assessment for 2018/19, scoring 90%. However, the online assessment was incomplete due to a suspected technical issue and is currently under review awaiting recompletion.

2.9 Policy and Procedure Updates

During 2018/19 the following policies and procedures that have IG content have been developed and/or reviewed, and then approved:

- ABMU Information Governance Procedures

- Freedom of Information Internal Procedures
- IG Breach and Near Miss Procedures
- NHS Wales Information Governance Policy
- NHS Wales Email Use Policy
- NHS Wales Internet Use Policy

Policies, procedures and guidance documents will continue to be developed or updated during 2019-20 to further support the IG agenda.

2.10 Information Sharing

ABMU shares information with various other organisations in order to provide safe high quality health care 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. A register of ISPs is reported to IGB bimonthly. During 2018/19, 23 information sharing agreements were developed and approved by the Caldicott Guardian or the IG team. In January 2019, the actions to refine and improve upon the development and recording of information sharing agreements and one-off disclosures were added to the IG Strategic Work Plan 2019-2021.

2.11 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 ABMU 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 teaches all staff about the need to complete a DPIA during mandatory IG training when conducted face to face, 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 IGB bimonthly.

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.

In February 2019, the action to review the effectiveness of these arrangements was added to the IG Strategic WorkPlan 2019-2021.

The DPIA templates were updated in February 2019 to take into consideration updated ICO guidance and to make them more user-friendly whilst still providing assurance that all IG concerns are covered. This update was done in partnership with the IT Security Department.

A summary of DPIAs managed during the period of 2018/19 are shown below:

- Approved 11
- In Progress 12
- Rescinded (no longer required) 21
- On hold (due to project reconsideration or Cyber Essentials Plus certification review) 9
- Awaiting submission 11

2.12 Boundary Change Support

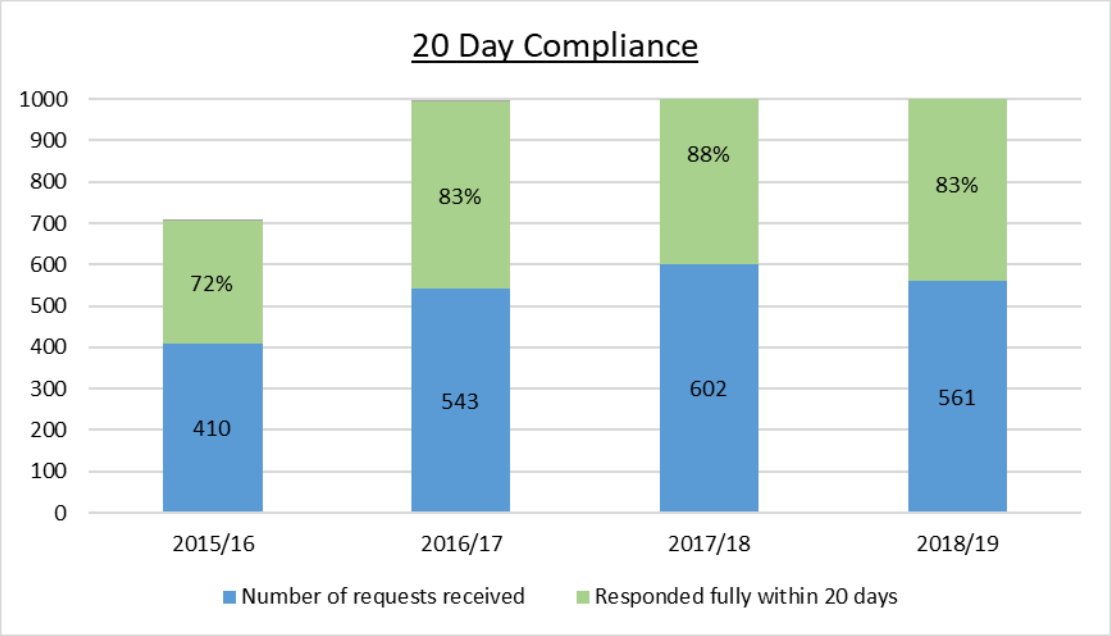
ABMU Health Board is required by Welsh Government to diseggregate some of its sites and services, due to move across to Cwm Taf University Health Board control on 1st April 2019. A great deal of IG work was undertaken in order to support this move enabling robust assurances to all concerned that data protection legislation and good practice would be followed throughout the process by both organisations involved.

2.13 Freedom of Information Act (FOIA)

Summary

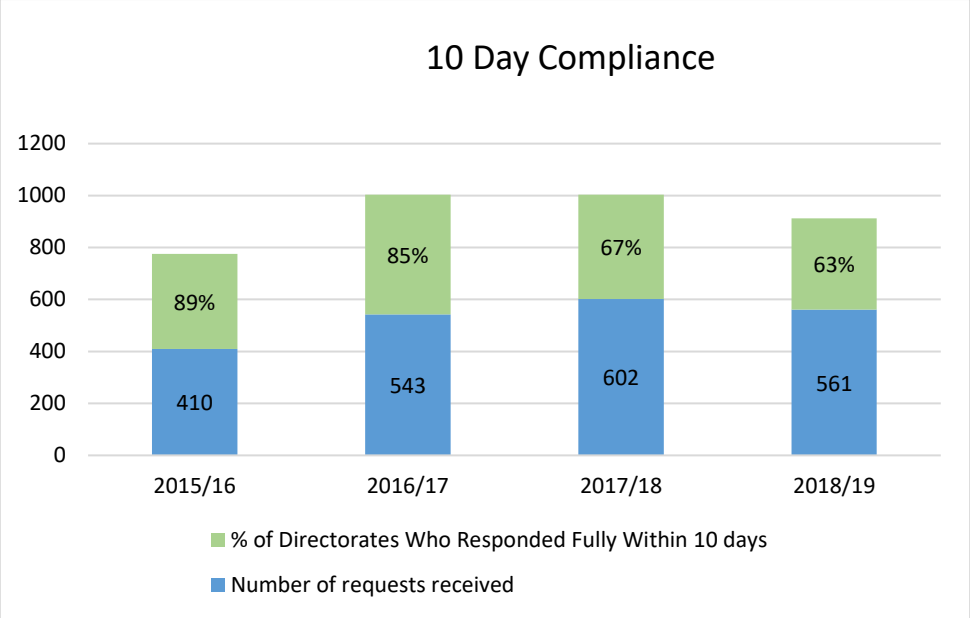
The Health Board received 561 FOIA requests in 2018/19. The Health Board answered 83% of these requests on time (within the 20 working days). Appeals about the Health Board's responses remain low (1%).

The graph below illustrates the Health Board's performance since 2015/16.



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 departments/directorate involvement. Having seen a decline in compliance over the past year we are continuing to closely monitor this.



Potential for Monitoring by the Information Commissioner

The Information Commissioners Office (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.

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 2018/19. Of these all 6 requests were upheld. There have been no investigations from the Information Commissioners Office (ICO) during 2018/19.

Decision	Number
Upheld	6

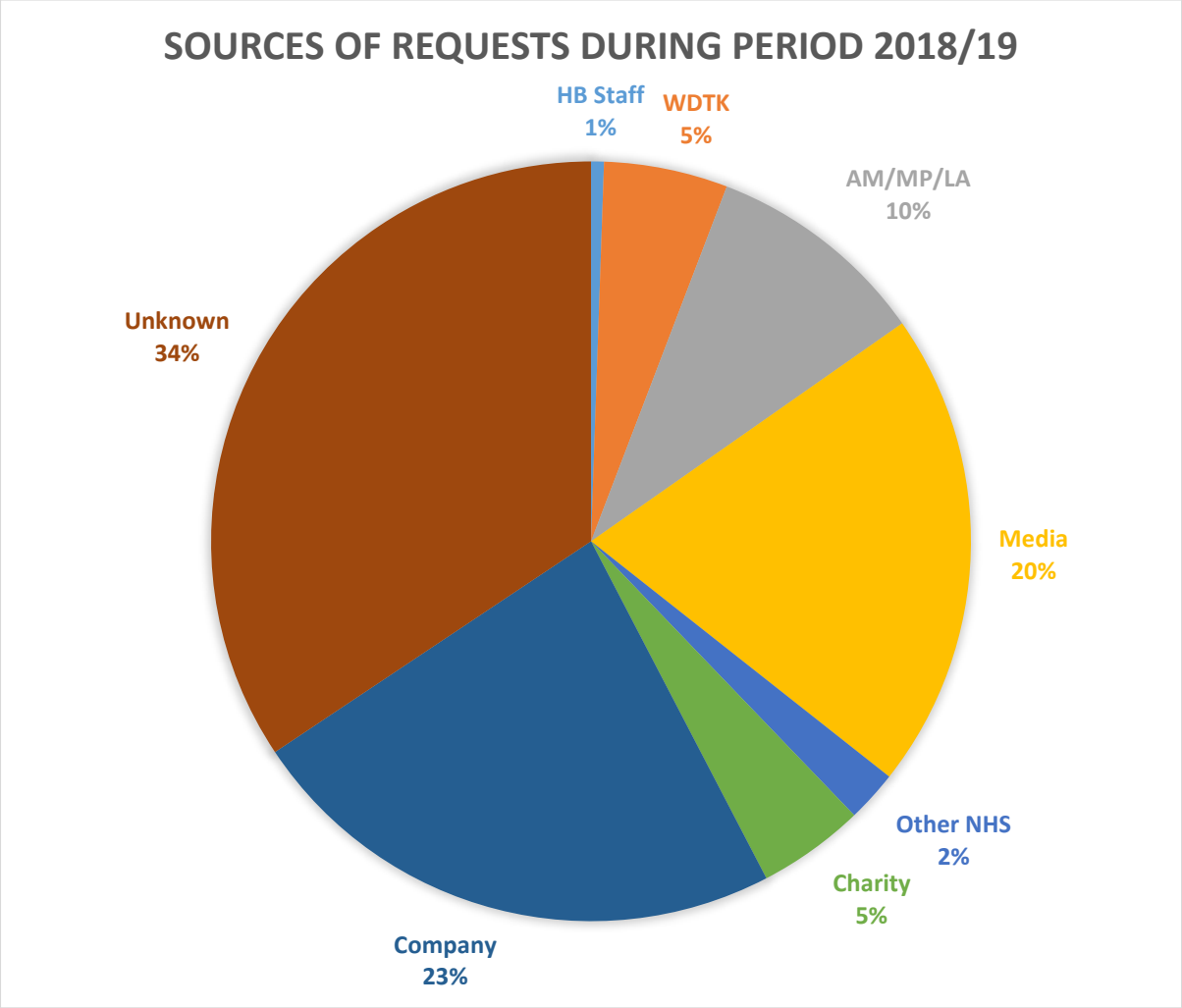
Request Trends and Subjects of Requests

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.)

Source of Requests

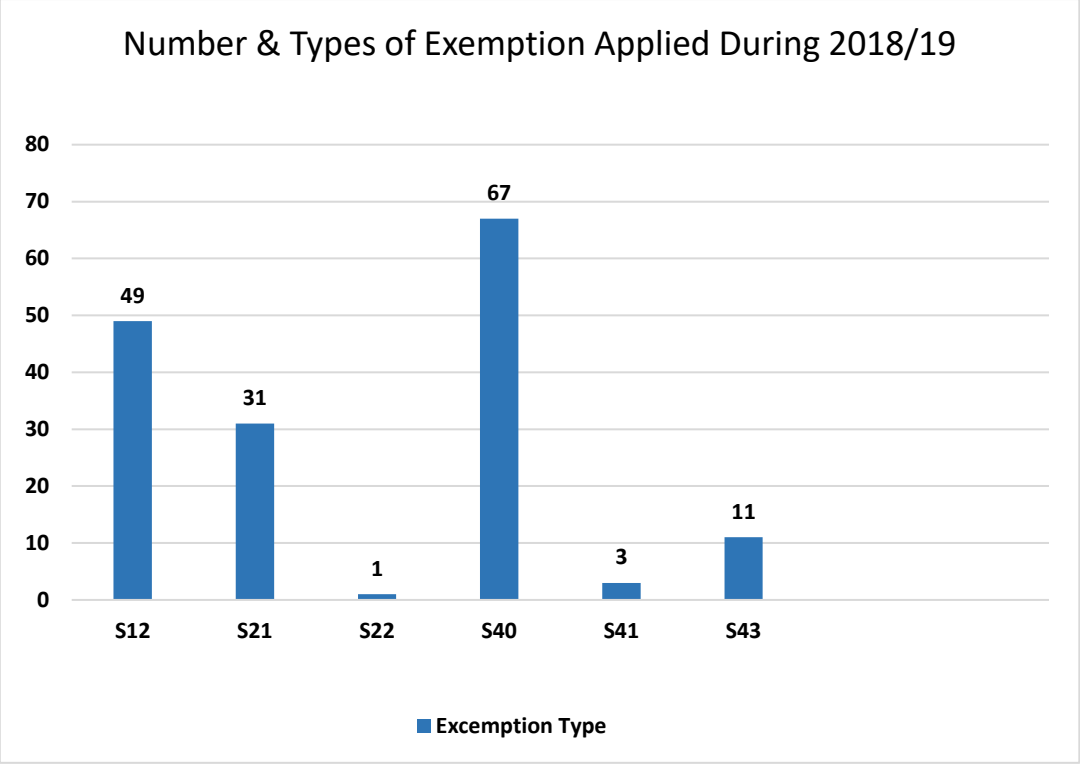
In accordance with FOIA, the Health Board maintains an 'applicant-blind' approach when providing information in response to requests. However, where that information is voluntarily provided by an applicant, the type of requester is recorded by the FOIA Team to help identify where the main demand for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

34% of all requests to the Health Board were made by sources not identified. 5% 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.



Transparency

The FOI Act carries an inherent presumption in favour of disclosure; information must be released unless one or more of the exemptions are engaged. From July 2017, the FOIA Team started to record the number of requests where an exemption has been applied. 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.
S40-Personal Information protected by the DPA / GDPR.
S41-Information provided in confidence (but only if this would constitute an actionable breach of confidence).
S43-Commercial interests.

2.14 Looking Forward – Plans, Priorities and Challenges for 2018/19

The IG agenda is wide and varied and therefore it is essential to have a planned and phased approach. The strategic actions for 2019/21 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 two 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 ABMU 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 2019/20 includes:

- Development of guidance documents in a number of IG areas such as data subjects' rights, data sharing and the recording of meetings;
- Production of a mandatory IG training video and its dissemination;
- Review of DPIA template and processes;
- Review of the use of smart / medical devices with regards to IG;

- Review of all Health Board policies to ensure data protection legislation compliance in other policy areas;
- Completion of the pilot Wales NHS IG Toolkit;
- Review Health Board IG Risk Register and utilise IGPG to actively manage the identified risks;
- Continue and finalise work on nationally agreed IG breach management guidelines; and
- Review and revise privacy notice templates and guidance.

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

SECTION 2 – CLINICAL CODING & HEALTH RECORDS

3.1 Clinical Coding Performance 2018/2019

Clinical coding information provided 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 have now set out new challenging targets from 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.
- 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.

ABMU Health Board has achieved the Year End Coding Completeness Target for 2018/2019, **attaining 99%** .There were 2873 uncoded episodes at Year End out of the total of 215,003 episodes, 2.5% more than 2017/18 (209,636 episodes).

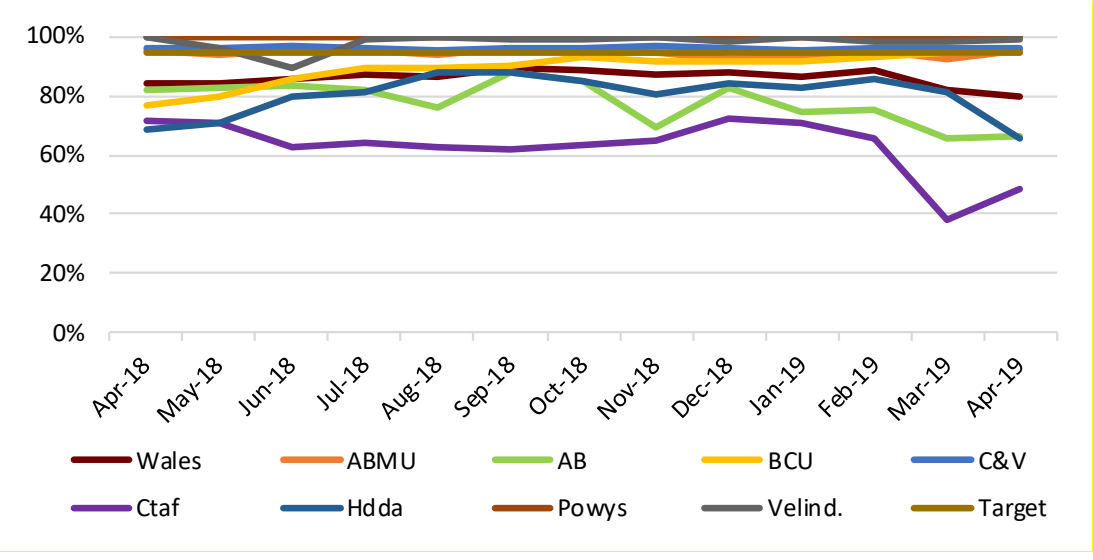
The data was submitted to NHS Wales Informatics Service (NWIS). Table 1 provides a breakdown of the 2018/2019 Year End position.

Table 1: Clinical Coding Completeness 2018/2019 - 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-18	16925	1079	94%	17381	182	99%

May-18	18292	1368	93%	18696	238	99%
Jun-18	17582	972	94%	18064	231	99%
Jul-18	18011	909	95%	18378	246	99%
Aug-18	17220	1321	92%	17676	271	98%
Sep-18	16829	730	96%	17137	175	99%
Oct-18	19252	954	95%	19349	203	99%
Nov-18	18668	2158	88%	18707	206	99%
Dec-18	16512	1523	91%	16540	310	98%
Jan-19	18720	1376	93%	18745	290	98%
Feb-19	16453	766	95%	16469	185	99%
Mar-19	17383	1401	92%	17861	336	98%
Totals	211847	14557		**215003**	**2873**	

Table 2 All Wales Clinical Coding position – demonstrates ABMU improvement and the sustained position in 2018/19



Source: NWIS Coding Extract June 2019

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

- Depth of coding was on average 4.7 during 2018/19, which was higher than the previous year of 4.6.
- Signs and Symptoms coding has decreased from 10.2% for 2017/18 activity to 9.97% in 2018/19 which in turn should result in more accurate quality information for reporting purposes.

The improvements and changes made in 2016/17 have been sustained in 2018/19 through the ongoing implementation of a detailed and robust improvement plan. During 2018/19 the Clinical Coding Department has continued to review ways of working, structures and processes to maximise the benefits of the increased funding received in 2016. The period has been a transitional phase, because the funding resulted in the recruitment of additional staff which required training and the development before the department was able to maximise the benefit of the additional resources.

In 2018/19 the Clinical Coding Department has benefited from an increasing number of productivity due to Trainees becoming more proficient in their coding abilities. One of the trainees who sat their exam in March 2018 passed both papers and became a qualified Clinical Coder, another trainee passed their practical paper exam which was sat in September 2018. The newest trainees have completed their training program and six sat their NCCQ exams in March 2019, four have passed both exams to become qualified Clinical Coders and two passed their practical paper exam so will be resitting their theory paper exam in the near future.

As more trainees become qualified Clinical Coders, this will decrease the assurance and learning functions of the supervisory team and provide further opportunity to increase quality and productivity. The supervisory team will ensure that they focus on quality of coding completed, 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 build on the achievements in recent years. Full plans and performance analysis are available in *Appendix S3a*

To support the ongoing improvement of the service a full programme of Clinical Coding Audit is carried out through the year, full details are available in the Coding performance information provided in *Appendix S3a*

3.1.2 The WAO Clinical Coding Review 2014 and Follow Up Review 2018

During 2014-15, the Auditor General reviewed the clinical coding arrangements in all relevant NHS bodies in Wales. That work pointed to several areas for improvement across Wales such as the accuracy of coding, the quality of medical records and engagement between coders, clinicians and medical records staff.

In October 2014 the WAO reported our findings for Abertawe Bro Morgannwg University Health Board (the Health Board) and concluded that ‘the Health Board recognised the importance of clinical coding and some of the associated processes

were robust, but more needed to be done to address the wider factors affecting accuracy and timeliness'. More specifically, it was found that:

- while the importance of clinical coding was recognised to some extent, more needed to be done to raise its profile and to focus on wider factors affecting its accuracy;
- some aspects of the clinical coding process were robust but clinical engagement was lacking, and the quality of medical records varied considerably; and
- Clinical coded data was used appropriately and was generally of a good standard, although some coding was inaccurate and timeliness had deteriorated the implications of which needed to be highlighted to the Board.

The report made recommendations that included a focus on

- Improve the management of Health Records
- strengthen clinical coding resources;
- further build Board engagement and resources; and
- Strengthen engagement with medical staff.

The WAO Clinical Coding Follow Up Review 2018

In 2018, the Welsh Audit Office conducted a follow up review to examine the progress made against the recommendations of the 2014 review.

The review concluded that the "**Health Board has invested in its clinical coding service, and the quality of its coded data is generally good. While the use of coding data as business intelligence remains underdeveloped, there has been reasonable progress in addressing previous audit recommendation.**

The considerable investment and service transformation that had happened in the Clinical Coding Departments was acknowledged. Area of good progress were identified in relation to the standards of achievement of two of the Welsh Government Tier 1 coding related targets, which NHS bodies are required to meet. These relate to completeness and accuracy. The accuracy target is that 95 per cent of hospital episodes should have been coded within one month of the episode end date. NHS bodies need to meet this target monthly rather than at the end of each financial year, which was previously the case.

- ABMU's performance has remained very close to the completeness target**. It has also been consistently above the average for Wales.**
- In terms of accuracy, NHS bodies are expected to show an annual improvement in their accuracy. Based on this review, ABMU's accuracy has improved (88.7% accuracy in 2014-15 compared to 91.21% in 2018-19) over time although there has been a slight deterioration in 2018-19.

The follow up of 2018 report noted that the importance of clinical coding has been recognised through new investment, which had contributed to sustained and improved performance, although the use of coded data for business intelligence is underdeveloped. It also acknowledges the efforts taken to revise management

structures and align Clinical Coding with Health Records and improve the support and management structure.

There are **no new recommendations** from the 2018 review; therefore, a new formal management response is not required. However as recommended the Clinical Coding department and wider Informatics Department will continue implementing its existing action plan and report progress through the Executive team via the Senior Leadership Group.

3.2 Health Records

3.2.1 Health Records Modernisation

A significant development during 2018/19 has been the initiation of the Health Records Modernisation Programme. The programme will implement a Radio Frequency identification (RFID) solution, with the objective of improving the clinical and logistical problems of a paper based health record. The programme will also modernise and improve the service.

The solution will provide RFID tagging of acute records, Location Based Filing using barcode scanning and identification of a patients records location, via fixed sensors. This will enable the record to be easily tracked, located, and made available when required.

During this period, additional staff have been appointed, to accelerate the retention and destruction programme, to maximise the storage capacity that is available across the sites. Nine storage areas have been mapped in readiness for the RFID technology, which equates to 82,000 shelves having IFIT labels. This piece of work took seventeen staff approximately twelve weeks to complete.

This mapping exercise will provide each shelf with a unique identifier, which will allow patients records to be filed within any space or shelf within the department (location-based filing). This will allow for greater efficiencies, thus maximising any available storage capacity within the library areas. The health records teams have also boxed and moved 70,000 inactive maternity records to Glanrhyd Hospital to create space for location based filing. This took twelve staff, two weeks to complete. During this period each of the library, areas have had thousands of notes validated, which has allowed less active records to be moved to off-site storage areas. The Senior Health records team have continued to work with IDOX, which is the supplier that will be implementing the RFID technology across the Health Board on cleansing the WPAS data in readiness for data migration.

There have been challenges with maintaining the storage capacity for RFID, due to the embargo that is now in place on the destruction of medical records across all Health Boards in Wales, as a result of the Infected Blood Inquiry. This has resulted in thousands of additional records having to be retained on an indefinite basis. The

Service has been able to secure an additional short- term storage solution within Unit 32, which is leased by the Health Board.

The Health Records Service will achieve efficiencies, through the introduction of RFID and the streamlining of working processes and will realise, a reduction in the Health Records establishment, by the 31st March 2020.

3.2.2 Ward Audit Programme

The Health Records full Ward Audit programme has ceased during this period due to the implementation of the Health Records Modernisation Project. In order to provide assurance the Health Records Senior Team continue to undertake records management audits where concerns have been raised in relation to records management practices. The team have continued to advise and provide professional guidance through these processes.

3.2.3 Towards a Digital Record

The service continues to work towards more electronic ways of working and less reliance on the paper record. The longer term solution to this problem it the availability of a full electronic clinical record for our patients. Progress continues across the Health Board with the rollout of systems, which will transform the way clinical information is captured, which will change health records practices across the Health Board. This is a critical step in achieving a digitally transformed organisation. Considerable work has gone into planning the Informatics three-year plan that describes the major milestone of the transition, progress during 2018 / 19 included

- **Patient Electronic Records** rolled out to patients via the Patient Knows Best platform. 727 patients signed up across 10 specialities and 50 clinicians, improving access to information to patients and freeing up valuable clinic appointments and improving communication
- **All-Wales View of Patient Diagnostic Results and Clinical Documents live and accessible in the Welsh Clinical Portal.** This supports regional working with Hywel Dda and the underpinning ARCH programme. During September 2018, 5% (6,000) of results reviewed by ABMU staff were analysed and reported on elsewhere in Wales i.e. 6,000 telephone calls/repeat tests avoided
- Electronic transmission of clinic letter to all GPs, improving communication about patient care and generating efficiencies.
- Clinical letter are created in the document Management System (DMS) available through the WCP and ABMU portal and can be accessed electronically in all clinical areas
- Electronic referrals – are available electronically through WCP and ABMU portal and can be accessed electronically in all clinical areas
- All GP practices can send Outpatient primary to secondary referrals electronically

- **Electronic Pathology Test Requesting implemented NPTH & Morriston inpatient wards.** 116 out of 240 locations live 48%, delivering improvements in patient safety - 91% reduction in patients bled unnecessarily in live ETR areas. Increased efficiencies – 40% reduction in average time for authorised full blood count results available in the record.
- **Access to the summary GP record** implemented across all sites; actively promoted through all implementations in clinical areas. This generates average time efficiencies of 32 mins of pharmacy time per admission. It increases patient safety i.e. pertinent clinical information is available sooner than was previously. It is now accessed 6000 times per month
- **SIGNAL, Electronic White Board Solution:** designed and implemented across Singleton Hospital, following success in Singleton Assessment Unit. Nursing Handover reduced by 30 mins, Doctor generating post-take list reduced from 45 mins to < 2 mins. No missing patient information. Access from anywhere in hospital. Improved IG compliance and team working. There was also increased digital readiness across all areas.
- **Community Mobilisation,** 100% of community staff (2400) now using an iPad to improve patient care and deliver efficiencies. Health Visitors mobile app to manage their caseloads and outcome appointments at the point of care additional 95 contacts per week.
- **Business Intelligence and Analytics.** There has been investment in market leading BI & analytics tools -QlikView & QlikSense. The recruitment of BI and Analytics Lead and a new information requesting management model. The roll out of management and patient support tools via the Ward Dashboard and Ward to Board Dashboard enabled through increased Data availability.

Digital records in 2019/20 and beyond

A full description of the plans for the next three years are available in the IMTP that supports delivery of the Informatics Digital Strategy to achieve Health, care and wellbeing activities carried out by everyone in our health economy will, with pace and scalability, be enabled using digital technology wherever optimal.

Some key achievements planned in 2019/20 will be the implementation of E-prescribing in NPTH and Singleton, roll out of digital nursing documentation in NPTH, currently a considerable paper legacy. Further readiness and improvement in-patient flow systems and information. Roll out of the Welsh Clinical Portal, the National Emergency Department System that includes the summary record available in WCP.

Work will continue locally to increase the number of professionals using DMS to increase electronic documentation, particular Allied Health Professional. Also effort will be put into ensuring departmental results such as lung function and endoscopy will also be available in WCP via DMS so that the need for paper filing is reduces and information is shared for clinical care. All of these development will further

progress the information available electronically and reduce the need for paper.

A key development in 2019/20 and 1920/21 will be the development of a solution that means no paper will be added to the record in the outpatient setting. Eventually this will mean (within 5 years of roll out) the majority of clinicians will not require the paper record in OPD at all. This will be achieved by the use of the electronic capture of information in OPD alongside the use of information already available electronically i.e. referrals, last letters and results. The electronic capture will be implemented in cancer specialities in quarter 4 of 2019/20.

Appendix

S2 – Clinical Coding

S2 - Appendix
Clinical Coding App

SECTION 3 – DATA QUALITY

4.1 The National Data Quality Performance Indicators

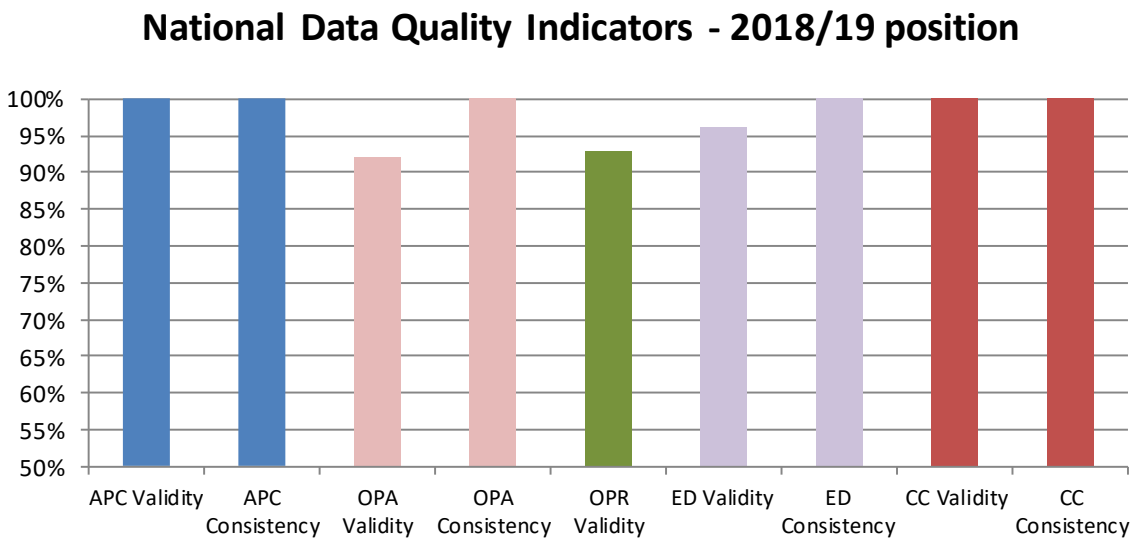
Good quality information is a fundamental requirement for the effective and prompt treatment of patients and to meet the needs of clinical governance, management information, accountability, health planning and service agreements. Poor quality data may not only affect a patient's treatment, but may also 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
- 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.

ABMU Health Board performance against these standards for data submitted within 2018/19 financial year is **98%**, achieving the required target for 272 of the 277 checks in place. ABMU are comparing extremely well alongside other Health Boards in Wales, as shown in the annual performance reports published by NWIS (*available in* A*ppendix S3a*).



A summary of the work undertaken to achieve this performance of 98% and reasons why ABMU did not achieve 100% performance for the Outpatient Activity (OPA), Outpatient Referrals (OPR) and Emergency Department (ED) data sets is set out in *Appendix S4a.*

4.2 Data Quality Improvement Work 2018/19

The Data Quality Team has continued to support services and new developments and drive forward improvements during 2018/19, 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 system developments e.g. Welsh Clinical Portal (WCP), Welsh Community Care Information Solution (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 ABMU on national data/system groups.
- Feedback to users to emphasise the importance of accurate and timely data.
- Daily adjustments on bed availability, ensuring occupancy is accurately reported both locally and nationally via the QS1 monthly submission.

Full details of achievements are available in Appendix S3b.

The team was centralised at Baglan HQ in April 2018, which was an important step towards developing the knowledge and skills further within the team, as well as ensuring that staff are supported on a daily basis.

4.3 Data Quality Improvement Plan 2019/20

For the period 2019/20 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 the Welsh Patient Administration System (WPAS), Welsh Community Care Information System (WCCIS), National Data Quality Indicators, Non Admitted Activity, Transgender & Adoption Process and EMPI will be progressed to further improve processes and data quality assurances.

The full description of the Data Quality Plan 2019/20 is available in Appendix S3b.

Appendix

S3 – Data Quality

S3 - Appendix Data Quality.docx

SECTION 4 – CYBER SECURITY

5.1 *Key Achievements in 2018/19*

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 and personnel information.

In May 2017 Cyber Security was brought to the forefront of everyone's attention within the National Health Service following the ransomware attack called Wannacry. This was a timely reminder that Cyber Security should be taken seriously and is essential for protecting services that increasingly rely on Information Technology.

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 hadn't applied these patches in a timely manner.

In 2017 a baseline assessment was commissioned by Welsh Government to assess the cyber position across 12 organisation 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, The Network and Information Systems Directive (NIS-D). Following this initial assessment by The Stratia consultants ABMU 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 ABMU 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 18/19 included a full patching regime was implemented across all PC, laptops and

servers within the Health Board for all Microsoft software. This was tested as part of the January 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.

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,
        3. Software with multiple versions e.g. 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.

c) Another area identified within the audit was the presence of old, unnecessary, unsupported software installed across the ABMU estate. To address this in 2018/19, 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 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 the SNOW asset management system.

d) It was highlighted that network vulnerability scans should be undertaken at least once every 6 months. It was reported last year that a number of national products had been purchased to address this issue, namely NESSUS vulnerability scanner and SIEM. This software will highlight vulnerabilities and provide alerts on security events (for example virus attacks, user account lockouts, firewall attacks etc.). To date these tools haven't been implemented within Swansea Bay due to complexity of delivering the National solution and the lack of Cyber security resources. Plans are in place for achievement in 2019/20.

e) **The network and Information Systems Directive (NIS-D) and related to the fact that data passing across local networks need to be encrypted to protect against inappropriate access and possible interception.** This is detailed as a priority for 2019/20, work has been ongoing with NWIS to prepare and complete assessments and plans as detailed below.

5.1.2 Network and Information Systems Directive (NISD)

NISD 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).

Welsh government is the competent authority under NISD 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 Welsh Government on how this will be implemented in Wales.

Progress in 2018/19 includes the preparation for the completion of the NISD Cyber Assessment Framework (CAF). 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. The assessment detailing the findings of the CAF will be provided to the Information Governance Group (IGG) in May 2019.

.

5.1.3 Infrastructure Improvements

During 2018/19 a number of improvements were made in respect to security on the network infrastructure. A significant improvement was made by implementing the authentication of medical devices, and allowing only access to areas of the network the device requires. This reduces the chance of a cyber security attack affecting the devices connected to the network using Wi-Fi.

In 2017/18 the next generation advanced firewalls were operating in “learning” mode and running in Monitoring IDS (Intrusion Detection System) mode. This was important to understand the flow of data across the network and not affect the running of clinical and administrative services by accidentally disconnecting them. Following this, as of March 2018/19 the firewalls are in “blocking” mode and IPS (Intrusion Prevention mode) which means that the firewalls are actively defending the network against any external attacks.

Assessment to further secure access to the Local Network is under consideration. Advances in technology in this area has continued and any solution going forward will require a business case which has capital and revenue implications. This is also applicable to medical devices and the Internet of things (IoT) devices.

5.1.4 Review of Vulnerable Infrastructure

During 2018/19 significant progress was made in identifying and replacing obsolete operating systems on desktop and laptops

- Windows 7 reaches end of life in January 2020. A migration project is in progress to upgrade all devices to Windows 10. Rollout of Windows 10 devices commenced in May 2017 and by March 2019 70% of laptops and desktop computers have been migrated from Windows 7 to Windows. A plan is in place to ensure the remaining devices are migrated to Windows 10 by January 2020.
- Microsoft Office reached end of life in October 2017. The migration to Officer 2016, at the end of March the programme is nearing completion. This will be completed in line with the timescales for the deployment of Windows 10.
- Windows Server 2003 instances – Significant progress has been made in removing Windows Server 2003 systems containing legacy applications. The ICT department are on course to meet the target date for removal of Windows 2003 servers by December 2019.

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.
483 services have been identified in the Service Catalogue at the end of March 2019.

5.1.6 Incident Management and Backup and Recovery

An Informatics incident response and business continuity plan has been developed and approved by the senior team. This document dovetails neatly with the organisation serious incident plan and the National Cyber Security Incident plan, it provides guidance on how to deal and communicate should an incident that affects IT services happen.

5.2 Development of strategy, capability, resources and operational priorities 2019/20.

The growing threat posed by Cyber Security requires a coordinated and sophisticated approach. To achieve this, a Cyber Security department will be established, the Cyber Security Manager post in the strucutre. The appointment is essential to provide strategic direction and strong leadership. The Cyber Security Manager will also be responsible for the development of policy, workload and action plans to ensure NIS, Cyber essentials, CAF asessment and the Stratia action plan are implemented across the Health Board. The manager will be supported by 3 members of staff who will be responsible for the security operational services, and technical implementation of security systems and processes.

5.2.1 Cyber Security

Stratia and NISD Key activities for 2019/20 will be the completion of the Stratia action plan and the development and implementation of the NISD action plan. The progress against the actions will be reported to the Information Governance Group and Service Management Group. The implementation plan will seek to address any gaps highlighted from the CAF in order to meet the set of 14 NIS Cyber security principles as required by the Competent Authority.

National Cyber Tools SIEM and Nessus implementation is planned for 2019/20. Although the implementation across the health Board will require dedicated resources this will be fulfilled once the appointments to the Cyber security department are completed. The install dates are expected to be implemented before the end of the financial year 2019/20.

Training A training package to raise awareness of cyber security has been made available by NHS Wales and the Health Board is seeking to make this training mandatory for all staff. The training package will be rolled out in 2019/20.

Anti Virus The current contract for Anti-virus software is due to expire in February 2020 a full procurement exercise will be run to replace this software in 3rd quarter 2019.

5.2.1 Maintaining Computer Systems

The ongoing maintenance of computer systems (networks, servers, desktop computers and laptops) continues to be a significant challenge. This is also important for protecting the organisation against known vulnerabilities for software that is no longer supported (updated). In 2019/20 work and resources will be identified in the Informatics IMTP (Intermediate Medium Term Plan) 2019-2021 to address:-

- Microsoft End of Life system refresh (e.g. 2008 and SQL Server 2008)
- Timely patching for networks, computers and servers
- Network End of life system refresh

Following on from the excellent work to patch Microsoft computers, work will focus on 3rd party software. This will include:-

- Removal of any software that is not required or doesn't meet Health Board requirements
- Identify an automated upgrade process for 3rd party software
- Provide additional controls for 3rd party software that cannot be updated automatically
- Implement process to stop unauthorised installation of software

5.2.3 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. still cause a significant challenge as they use software that in may not be able to be patched or

upgraded due to their FDA compliance for example. During 2019-2020 a control process will be rolled out for all new installations which will need to be completed prior to installation.

Following a recent proof of concept a preferred supplier was identified for network analysis software. A bid for the preferred option has been submitted to Welsh Government for the network monitoring system. If the bid is turned down then a business case will be developed and submitted to the Investments Benefits Group (IBG) in due course.

5.2.4 Asset Management

The IT Asset Management Improvement plan is now in its second year. Planned key improvement for 2019/20 include

- improving the Starters and Leavers process,
- Software license harvesting process which will reduce unnecessary purchasing of software.
- Creation of a detailed asset dashboard that will inform software and hardware refresh lifecycles