SECTION 1 - INTRODUCTION BY THE SENIOR INFORMATION RISK OWNER

It is a great pleasure to present ABMU's second 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 2017/18 the governance models and structures for the management of Information Governance in ABMU were strengthened and have matured. The role and influence of the Information Governance Board significantly increased. There is good evidence that robust Information Governance practices have been embedded across the organisation. During 2017/18 there was significant preparation work completed in readiness for a changing legal landscape. Much of the Information Governance activity during the period was in preparation for the Introduction of General Data Protection Regulation in May 2018 and the Data Protection Act 2018. The commitment of the Health Board to good information governance was demonstrated with an increase in resources for the Information Governance Team to prepare for GDPR and then maintain and improve practices across the Health Board.

The General Data Protection Regulation (GDPR) was approved in 2016 and came into force on 25th May 2018. It is directly applicable as law in the UK. It replaces the Directive that is the basis for the UK DPA, which will be repealed or amended. It is

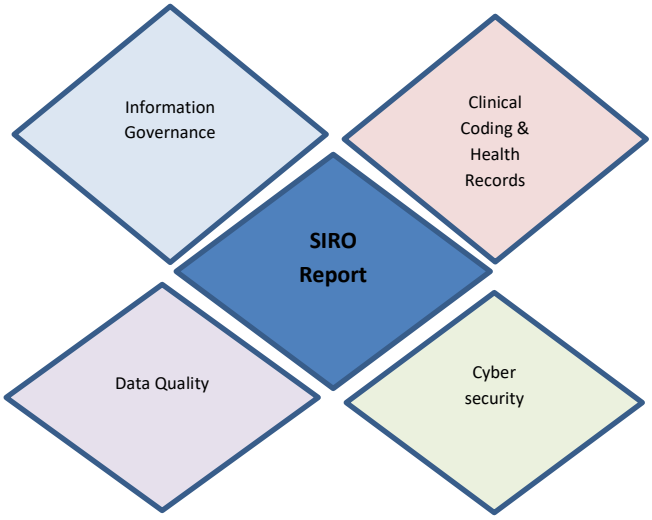
expected that the provisions of the GDPR will remain in force post-Brexit, and for the foreseeable future.

Although in general the principles of data protection remain similar, there is greater focus on evidence-based compliance with specified requirements for transparency, more extensive rights for data subjects and considerably harsher penalties for non-compliance.

The GDPR introduces a principle of *'accountability'*. This requires that organisations must be able to *demonstrate compliance*. The key obligations to support this include:

- The recording of all data processing activities with their lawful justification and data retention periods;
- Routinely conducting and reviewing data protection impact assessments where processing is likely to pose a high risk to individuals' rights and freedoms;
- Assessing the need for data protection impact assessment at an early stage, and incorporating data protection measures by default in the design and operation of information systems and processes;
- Ensuring demonstrable compliance with enhanced requirements for transparency and fair processing, including notification of rights;
- Ensuring that data subjects' rights are respected;
- The provision of copies of records free of charge, rights to rectification, erasure, to restrict processing, data portability, to object, and to prevent automated decision making;
- Notification of personal data security breaches to the Information Commissioner; and
- The appointment of a suitably qualified and experienced Data Protection Officer.

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 2017/18 and sets out the priorities and plans for 2018/19, in the following areas.



- **Section 2**, Information Governance provides comprehensive evidence of the work programme undertaken to prepare for the implementation of GDPR, and demonstrates across all areas improved assurance and compliance. Examples of progress include an improved Caldicott in Practice self-assessment score, improved training compliance, the development and implementation of the Individual Asset Register (IAR) the previously lack of the IAR was a well-documented risk that has now been addressed.

  During this period the ICO performed a desk based follow up audit in September 2017 following their full audit in 2016, with 190 documents submitted as evidence. The ICO's follow up report is summarised in the report and the Health Boards improvement was acknowledge.

- **Section 3**, 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 Records section describes the significant investment in Health Records service planned for 2018/19, to modernise the management of the library services with the introduction of RFID technology to track records and change the way the service is delivered and deliver operational and organisational benefits.

- **Section 4**, Data Quality presents the ABMU Health Board performance against the Data Quality standards for data submitted within 2017/18 financial year. ABMU achieved 98**%**, achieving the required target for 268 of the 273 checks in place. ABMU 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 5**, 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.

Conclusion

Information Risk and Information Governance must be the business of every one if the Health Board is to meet the expectations placed upon it by Government, the Information Commissioner, patients and staff. This will be a challenging year as the Health Board meets and responds to the demands of on the new General Data Protection Regulations (GDPR) from May 2018.

SECTION 2 – INFORMATION GOVERNANCE

2.1.1 Accountability / Responsibilities and Governance Structures

In February 2016, the Health Board asked the Audit Committee to provide it with assurance regarding Information Governance (IG). An Information Governance Board (IGB) was established, 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 provides reports to the Audit Committee.

By early 2018 the Executive team recognised the need for considerably increased resources to be given to the IG Department which resulted in a notable and successful recruitment drive. The IG Department is now fully resourced and is in a very strong position to deliver the operational Work Plans and 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 changes in May 2018 with the introduction of the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. The Strategy aims to prepare the Organisation for the introduction of the new data protection legislation, and will be reviewed as details of the new legislation become clear.

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 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 Senior Information Risk Owner (SIRO) in July 2017, to be superseded by the Director of Corporate Governance / Board Secretary in July 2018. The Board Secretary became the Deputy SIRO, to be superseded by the Assistant 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. The Deputy Medical Director is the Deputy Caldicott Guardian.

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;
- Investigating 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 Assistant 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 deliver 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 is 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 builds on previous privacy and data protection legislation but intends 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 informs the new DPA 2018 which also comes 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 will not change, and will provide a solid foundation post May 2018. ABMU already have sound and strong professional practices, which will be reviewed and further built upon to ensure ongoing compliance with the new data protection 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 needs 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. The historical low level of resources within the IG Department led to an unsatisfactory position in the months preceding the new data protection legislation:

- Of the 59 individual tasks on the GDPR Work Plan, the Health Board was only fully compliant in 8 by the end of March 2018, although a further 17 areas were anticipated to become compliant by May 2018 when the new legislation came into place.
- Of the 12 areas noted by the ICO, by the end of February 2018, ABMU was compliant in 1, however compliance was anticipated to be achievable in 5 areas of the 12 by May 2018 when the new legislation came into place.

It is anticipated that of the 59 individual tasks, ABMU will be fully compliant in 50 of these by the end of 2018 due to the increased IG staffing resources now in place. 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, an annual plan has been agreed, alongside the specific GDPR Work Plan. 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:

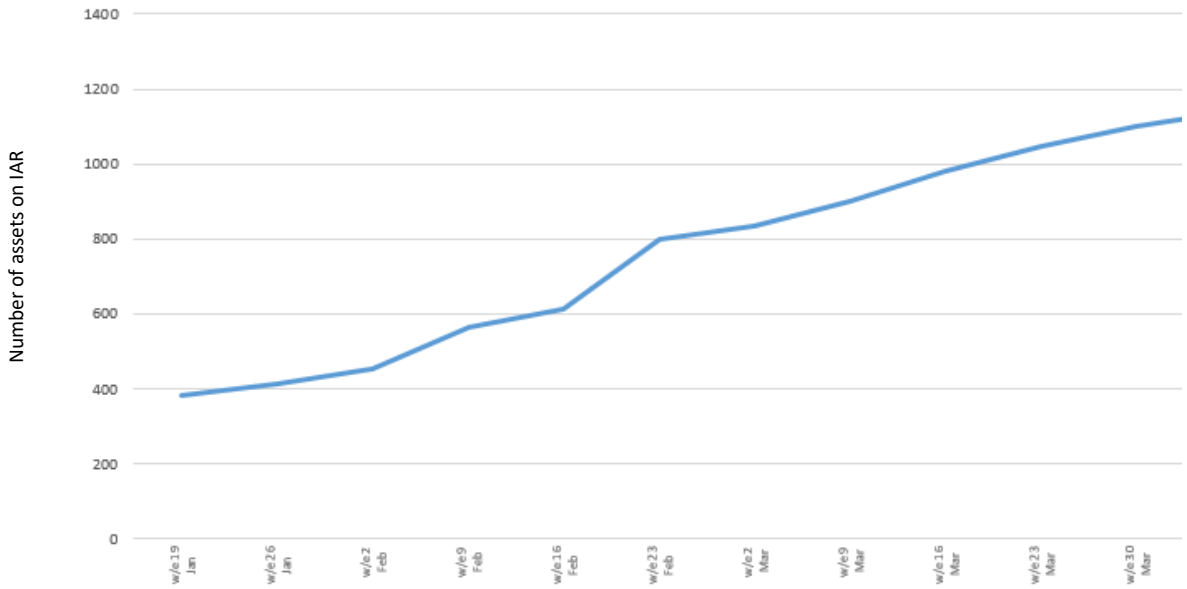
> *'An identifiable asset owned or contracted by an organisation which is of value to the business. It will include databases, applications, technical computing infrastructure, paper record stores, and policy/process/ educational related materials'.*

One of the most important strands of work for this financial year has been the ongoing development of a useful and robust IAR.

An IAR User group was established in order to offer practical advice and support to the IGB Leads, and to encourage best practice around the Health Board's information assets. The User group meets every quarter and is well attended.

Two temporary agency staff were employed in mid January to assist with data entry into the IAR. They developed an excellent working relationship with the IGB Leads, offering practical advice and support to Heads of Service and nominated Infortmation Asset Owners (IAOs) in the Service Delivery Units / Corporate Directorates. This extra

input resulted in a significant increase in assets catalogued. This growth is shown below:



The IAR is held on SharePoint which allows for detailed reporting as well as access by the IAOs to actively manage and audit their information assets.

2.4.2 Subject Access Compliance

Patient Subject Access Requests

The total number of patient Subject Access Requests (SARs) for the financial year 2017-2018 was 5282. This is an average of approximately 440 per month which is slightly lower than 2016/2017. The largest proportion of requests continues to be those received from solicitors. However, the department has seen a considerable increase in the number of requests received during this period for requests made by Government Agencies for patients' information.

The compliance rate of meeting the 40-day provision requirement at March 2018 was **99.9%,** which maintains the high performance seen across the Health Board since the service was consolidated into a single 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	99.9%
Government Agencies - 10 days				
15/16	**925**	**925**	**0**	**100.0%**
16/17	785	785	0	100.0%
17/18	**1797**	**1797**	**0**	**100.0%**

Following an incident in 2015 of disclosure of information about a third party to a SAR requestor, the department developed and has continued to implement 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 2017/2018 there were 65 reported incidents up until March 2018.

For the year 2018/19 the Subject Access Department have implemented a new way of working to ensure all processes and provision of records comply with the new GDPR regulation from the 25th May 2018. This includes patients who request copies of their records electronically, they can now receive these electronically following the process that has been in place prior to May 2018, for releasing information securely to Solicitors and the Police. A fee can no longer be charged for providing patients records with a projected loss of income of approximately £170,000 per annum.

Staff Subject Access Requests

For 2017/18 the Health Board processed a total of 14 Subject Access Requests for staff. Staff SAR requests are managed through the Workforce and OD Directorate and in this year some internal resources were allocated on a temporary basis to lead on SAR as the complexity of the work could not be absorbed by the existing teams. In many cases the breadth of information sought, particularly from email systems, is our greatest challenge. The team are currently looking at making the resource allocation

to SAR support permanent for this reason. A revised Staff SAR Policy is being developed and is aimed to be in place Q3 2018/19.

2.4.3 Information Governance Training

The IGB has made IG training compliance a priority, setting a target of 95% overall compliance by the end of 2017/18. Although this target has been missed, significant improvement was made during the year. At the end of 2017/18 the Health Board stood at 60% overall compliance, an 87.5% 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 targetting of individual non compliant staff or poorly performing departments. Poorly performing 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 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;

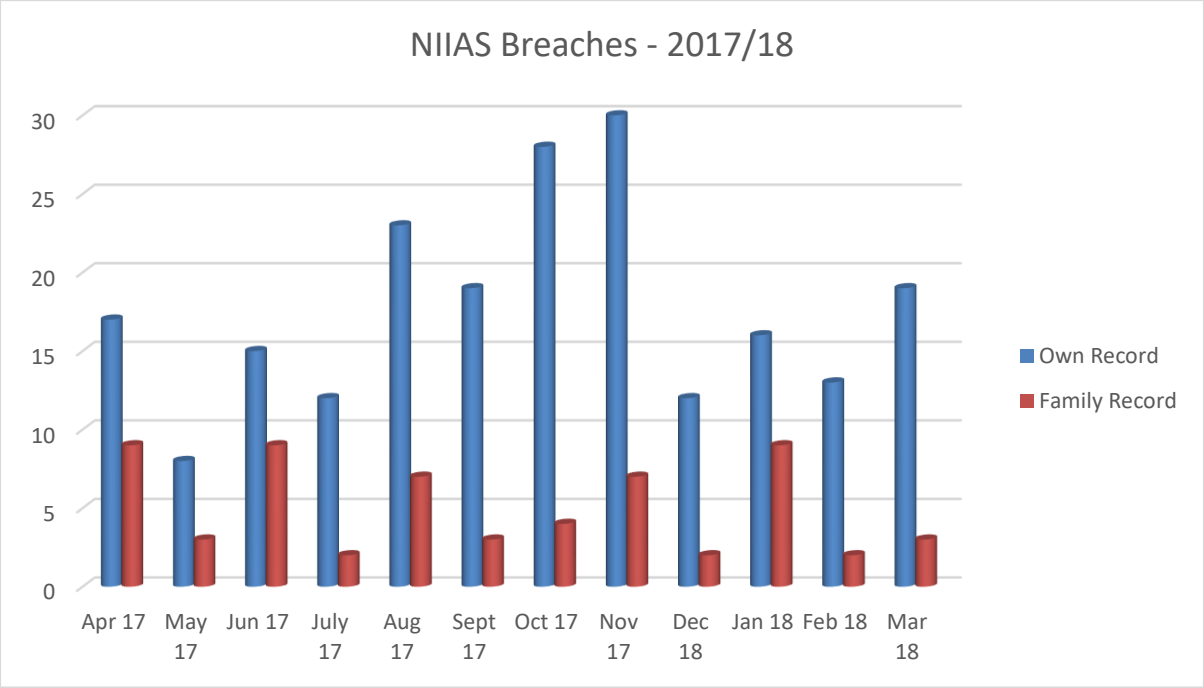
- AAA / Bowel Screening;
- Welsh PAS;
- CANISC;
- ESR;
- Welsh Demographic Service;
- eMPI;
- Choose Pharmacy; and
- WEDS.

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

- WLims; and
- 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 are shown below, where incidents picked up by NIIAS were consequently confirmed as inappropriate access:



There are fewer confirmed incidents than in many other Health Boards. Incidents are reported to the IGB monthly 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 2018/19.

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 five main types of audit:

1. ICO – external follow up General Audit;
2. ICO – external follow up Training Audit;
3. Wales Audit Office follow up Audit;
4. Internal Audit follow up Audit; and
5. IG Department led Audits.

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

2.5.1 Information Commissioner's Office (ICO) follow up General Audit

In September 2016, ABMU agreed to a consensual audit by the ICO of its processing of personal data. The ICO were sent hundreds of documents as evidence of practice in ABMU prior to their arrival on site for three days. The audit scope included:

a) Data Protection Governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the Organisation;
b) Records Management – The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records; and
c) Data Sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the DPA and the good practice recommendations set out in the ICO's Data Sharing Code of Practice.

The audit provided limited level assurance that processes and procedures are in place and delivering data protection compliance. The audit identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA. There was one reasonable (Health Records Management) and two limited assurance assessments where controls could be enhanced to address the issues which are summarised below.

Areas of good practice were identified that included:

- Although not mandated by NHS Wales, ABMU have appointed a SIRO to ensure greater oversight of Information Risk across the Organisation;
- Monthly audits and spot checks are completed, to monitor how records are being tracked, logged and stored. Quality and accuracy checks are also done monthly. The results are then fed back to each department. If there are any recurring issues or breaches, extra training will be provided to the relevant staff members; and
- There is a comprehensive intranet site dedicated to Data Protection and Confidentiality with guidance and links to relevant policies, aimed at promoting awareness of staff responsibilities towards data protection compliance.

The ICO performed a desk based follow up audit one year later in September 2017, with 190 documents submitted as evidence. The ICO's follow up report is summarised below:

ICO Follow Up Audit Report 2017
Main Improvements
1. The ICO acknowledges the progress made by the Trust to improve compliance in the areas audited, and in particular: • An Information Governance Strategic Direction and Framework for 2017 – 2020 has been drawn up to support and drive the effective management of the information held by ABMU • Development of an Information Asset Register (IAR) is well underway. An IAR user group has been established, and training is being arranged for Information Asset Owners (IAOs), Information Asset Administrators (IAAs), Information Governance Board (IGB) Leads, and will cover the identification and registration of information assets • The IAR will contain all data sharing agreements, the legal basis for sharing and the name(s) of responsible officers. Steps have been taken to raise awareness among staff of the need to notify the Data Protection and Confidentiality Department of any information sharing agreements • Key Performance indicators (KPIs) are now reported at IGB meetings with shortcomings discussed and followed up • Work is underway to formalise the requirement to carry out Privacy Impact Assessments (PIAs). A template has been developed and publicised along with information for staff on the need to carry out PIAs • National Intelligence Integrated Audit Solutions (NIIAS) compliance reports have been presented to the IGB. The IG department are monitoring how well line managers respond to NIIAS notifications which are sent to them • A 'Health Records and Clinical Coding Business Continuity Plan' has been drawn up and approved by the Audit Committee
2. Security improvements have been noted as follows: • Action has been taken to highlight the importance of locking computer screens. ABMU is also looking into possible secure sign-on solutions • The IG audit procedure includes checking whether there is inappropriate staff or patient information on the white boards in the wards • Improvements to security have been made at one of the record libraries by key codes being added and a door to a car park no longer being used except in an emergency, and covered in reflective glass

Areas still outstanding Within the scope areas there are still a number of recommendations which have yet to be progressed to completion:
1. Work is ongoing to establish procedures for dealing with one-off disclosures, with the development of a one-off disclosure log. Draft procedures have been produced for releasing information to the police
2. There is not room in the budget for ABMU to introduce lockable trolleys and it is not possible to provide covers given the design of the trolleys. We would recommend that the transferring of records in unlocked trolleys continues to be identified and monitored as a risk. It would be good practice for any new trolleys purchased in the future to be lockable
3. A new version of the Patient Administrative System (PAS) is to be introduced in November 2017, and staff have been asked to attend training sessions with a reminder that non-compliance with training could impact access rights. We recommend that the attendance at these sessions is closely monitored and that refresher training at regular intervals is similarly managed
4. Several of the recommendations made by the ICO involve the updating of ABMU's Data Protection and Confidentiality Policy. A national data protection policy is being developed and ABMU will be represented on the working group and use the ICO recommendations to inform their input. However it appears that the national policy has been delayed, and an interim policy is to be developed by ABMU. We would recommend that this is done without undue delay
5. ABMU have put procedures put in place to meet the actions in a number of recommendations; however these are not able to be completed until the IAR is fully populated
6. Several recommendations concerning data sharing have not yet been carried out as they are dependent on the IAR being fully populated. These relate to the implementation of periodic audits or dip checks to ensure the accuracy of data and the destruction of data in line with agreed retention periods
7. ABMU have accepted the need for an Information Risk Policy but are prioritising work on the IAR instead. There is a planned completion date of July 2018, and we recommend that ABMU ensure that the stated dates are kept to
8. No progress has been made concerning the review of consent aspects of clinical training sessions due to resourcing issues. We would recommend that this is implemented in a timely manner. This will be taken forward as part of the GDPR action plan in 2018/19.

A new Information Governance Policy was ratified in early 2018 and checks are made that staff have read and agree to this Policy. As noted in section 2.3.1, excellent progress has been made with the IAR. Any outstanding items are part of the Work Plans currently being actioned by the IG Department and across the Health Board, and closely monitored by the IGB.

The ICO published the following statement on their website, to evidence that a follow up was carried out:

> "The ICO has carried out a follow-up of the data protection audit performed at Abertawe Bro Morgannwg University Health Board with its consent."

The full report is not published on their website, nor is the notable progress made by ABMU reported publically in any way. The audit engagement is now complete.

2.5.2 Information Commissioner's Office follow up Training Audit

The ICO conducted an audit into IG Training across NHS Wales in 2015, and their follow up took place in October 2017. ABMU's response included the submission of 116 documents as evidence. The ICO commended ABMU on the completion of all actions in the 2015 audit. The ICO reported separately to Welsh Government with strategic recommendations to work to improve training compliance across NHS Wales in general.

2.5.3 Wales Audit Office (WAO) follow up Audit

The WAO audited the IG Department as part of a wider IT Infrastructure follow up Audit in November 2017. They stated at the time that further progress had been made in the previous year than had been anticipated, but that the state of IG resourcing would render ABMU as not being able to adequately prepare for GDPR implementation by May 2018. This view contributed towards the recognition that the IG team needed to be considerably expanded.

2.5.4 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.

2.5.5 IG Audit Programme

The IG Audit Procedure was developed and implemented from February 2017. A walk around of Singleton, PoW, Morriston and NPTH was undertaken in the first instance and departments volunteered to be audited at that time. The IG Department also prioritised areas flagged up by the ICO during their audit as non-compliant, as well as those areas that had recent Datix noted breaches.

The IG Audit Programme was planned for the 2017/18 financial year and the IGB received regular audit updates, from which IGB leads were expected to ensure completion of action / improvement plans. IGB Leads were asked to help prioritise areas that would benefit from an IG Departmental Audit. Any ICO reportable breach would trigger an IG audit of the relevant department, as would any repeat lower level incidents.

IG Department Audits are 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)

Initial IG audits conducted during the financial year 2017/18 are summarised as:

- 5 areas audited rated Green
- 7 areas audited rated Amber
- 2 areas audited rated Red

All areas rated yellow and red are followed up at an appropriate time, and follow up audits within the period 2017/18 are summarised as:

- areas followed up rated Green
- areas followed up rated Amber

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 on information governance 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. Incidents are managed as part of the local SDU / corporate governance assurance process and are escalated to the IG Department for guidance and support where required.

The exact number of confirmed information governance incidents reported during the period 2017/2018 cannot be determined at this time due to changes made to the reporting categories within the Datix (incident reporting) system. To alleviate this

problem in future and support timely compliance with GDPR requirements for the reporting of data breaches, functionality has been established within Datix to enable those reporting incidents within the organisation to notify the IG Department of any IG related breaches. This will allow for more robust reporting and assessment of data breaches and the ability to produce Datix reports that are not solely reliant on using reporting categories.

During the reporting period three incidents were deemed to be of a severity level requiring self-reporting to the ICO. These three incidents are summarised below:

- In May 2017, patient information was found in the vicinity of, and within, an unoccupied building that had been decommissioned by the Health Board;
- In May 2017, a file containing referral information about five children was identified as missing within the Speech and Language Therapy Offices; and
- In June 2017, an incident was reported after it had been identified that information about a complainant had been misfiled in another complainant's record and shared incorrectly with the first complainant's family and the Ombudsman.

Each of these incidents has been fully investigated by both the Health Board and the ICO, with remedial actions and improvements undertaken swiftly. The ICO took no action, and has received sufficient assurances to consider these incidents closed.

There were two complaints made to the ICO during 2017/18 requiring ABMU investigation:

- In October 2017 a patient stated that ABMU did not comply with their request to alter their medical record. The ICO investigated and found no breach of data protection legislation and the case was closed;
- In November 2017 a patient stated that ABMU had lost their maternity record and had not taken suitable steps to remedy the situation. The ICO investigated and found that ABMU had breached data protection legislation, but had taken suitable steps since to both remedy the situation and to put processes in place to prevent a similar incident occurring in the future. They therefore took no further action.

The process and procedures used to ensure the appropriate management, assessment and reporting of all IG breaches, irrespective of reporting to the ICO, is under review to ensure compliance with the requirements of new data protection legislation.

2.7 Information Governance Risk Register

The Health Board IG Risk Register is assured by the IGB. Due to resourcing issues within the IG Department these risks have had limited attention this financial year. Resourcing has since been addressed and the risks will be reviewed and action plans

put into place during 2018/19. The IAR will also be used to assess risk and the Work Plans reviewed accordingly with the aim of mitigating risks.

By March 2018 the risk register identified 20 risks that score between 9-20. The themes on the Risk Register included:

- Low mandatory training compliance;
- Information sharing and release to third party;
- Asset management and register;
- Breach and Incident Mangement;
- Readiness and adherence to GDPR;
- Insufficient Resources;
- Staff Subject Access process;
- Poor practice and coodintaion of release of information to the Police; and
- Implementation and adherence Privacy Impact Assessments.

Due to the level of risk, the importance placed on effective management of infomation and the high profile nature of the potential fines from the ICO, two risks remained on the Corporate Risk Register: Insufficient IG resourcing and low mandatory IG training compliance.

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 2017/18, scoring 91%, giving it the maximum total achievable rating of four stars.

An Out-Turn Report has been produced and will be taken to IGB in September 2018, although all actions necessary had already been identified and form part of the GDPR Work Plan monitored by IGB on a bimonthly basis. The actions to be taken during 2018/19 that will further improve the CPIP score are:

- Better manage patient preferences
- Identification and review of locally drawn up contracts
- Further work on local tier 3 privacy notice development
- Training to be made available for short term contract and locum/temporary staff
- Review of confidentiality clauses with employment agencies
- Continued drive for increased levels of IG training compliance for staff
- Continued work on Information Asset Register
- Information Asset Owners to formally monitor the management of their assets

The 2016/17 SIRO report noted several areas of prioritisation resulting from the CPIP submission. All areas are monitored by the IGB bimonthly, and an update is shown below:

2016/17 area for improvement	**2017/18 position**
To increase levels of IG training	Compliance has improved from 32% in March 2017 to 60% in March 2018, an increase of 87.5%. ABMU's target remains at 95% and the drive to reach that target continues
To improve the security and privacy of patient information	ABMU continues to improve and this target is being approached by several different routes, all monitored via the GDPR Work Plan
To increase and improve upon information sharing arrangements and improved central management	ABMU now has an Information Asset Register which is being used to improve the management of all information sharing
To improve the information security event reporting and management procedures have been communicated to staff/relevant third parties	A procedure has been developed to better manage all breach reporting and management, and contracts with third parties are under review
To develop a robust IG audit programme	An IG Departmental Audit programme was started back up in January 2018 and includes planned and unplanned audits, concentrating on high risk areas and those who have had an IG breach

Implement guidance and awareness for staff on the use of Privacy Impact Assessments (PIAs)	Data Protection Impact Assessments (formerly known as PIAs) were a mandatory requirement within ABMU by the end of the 2017/18 period
To improve the way the Health Board provides patients and the public with information, about how their information might be used via privacy notices which are published on the Health Boards website	Tier 1, 2 and 3 privacy notices for patients and staff were in advanced development by the end of the 2017/18 period
Improvement management and escalation of Information Risks and breach reporting	Risks and breaches are formerly reported to IGB, and many of the risks are already being actively managed and reduced as part of the GDPR Work Plan

2.9 Policy and Procedure Updates

During 2017/18 the following policies and procedures that have IG content have been developed, reviewed and approved:

- Information Governance Policy;
- Fax Policy;
- Health Records Disaster Recovery Policy;
- Decommissioning Policy;
- Adoption Policy;
- Medical Devices Backup Guidance; and
- Police Disclosure Procedures.

Policies and procedures will continue to be developed or updated during 2018/19 to further support the IG agenda. The IG community in Wales is taking a collaborative approach and many policies are now being developed 'once for Wales', including a national IG Policy, an Information Security Policy and an Information Risk Policy. Once these are in place, ABMU will produce a local IG Procedures document, to be approved by IGB and the Audit Committee as necessary.

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 the 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 2017/18, 3 national audit and 22 information sharing agreement / disclosures were developed and approved by the Caldicott Guardian or the IG team. Now that the IG team is fully resourced, alongside the IAR completion, the development and recording of information sharing agreements and one off sharing will be refined and improved.

2.11 Data Protection Impact Assessments (DPIAs)

During 2017/18, ABMU rolled out the completion of DPIAs across the Health Board, thereby ensuring that IG and security are embedded in new information flows from the outset.

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 with technologies and processes that are 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.

A summary of DPIAs managed during the period of 2017/18 are shown below:

- Approved 6
- In Progress 3
- Rescinded 1 (no longer required)

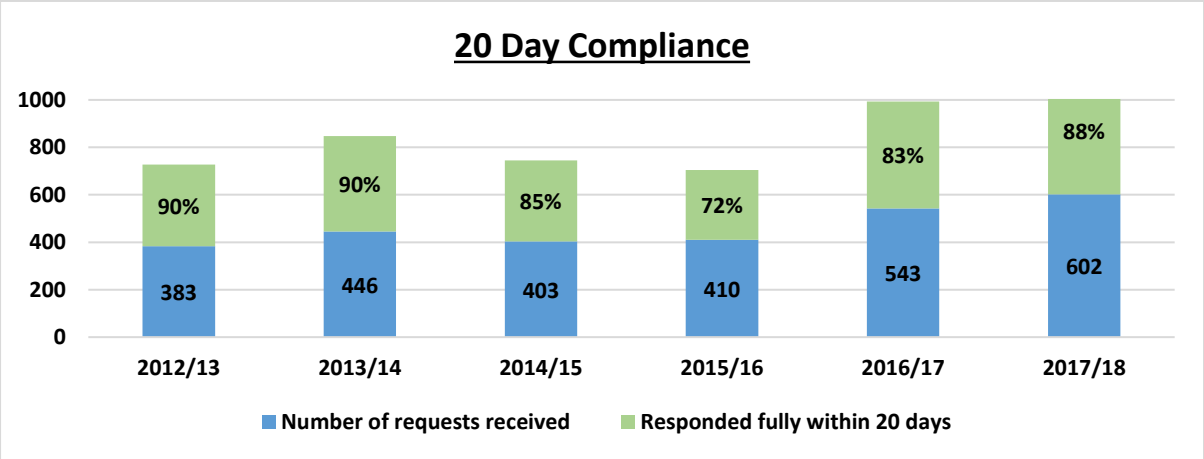
This period was one of the Health Board learning a process before it became a legal requirement, alongside minimal support services available due to resourcing levels within the IG Department. The Health Board now has a proactive DPIA Lead in place, and it is anticipated that 2018/19 will have a far greater number of DPIAs actively supported by the IG Department and Information Security, completed and recorded, thus reducing the risk associated with new flows of information.

2.12 Freedom of Information Act (FOIA)

FOIA requests are handled by the Corporate Department within ABMU.

The Health Board received 602 FOIA requests in 2017/18; this represents an increase of 10% on 2016-17. The Health Board answered 88% of these requests on time (within the 20 working days). Despite this increase in the number of requests, appeals about the Health Board's responses remain low (1.33%). One appeal was referred to the Information Commissioner's Office (ICO) during 2017/18.

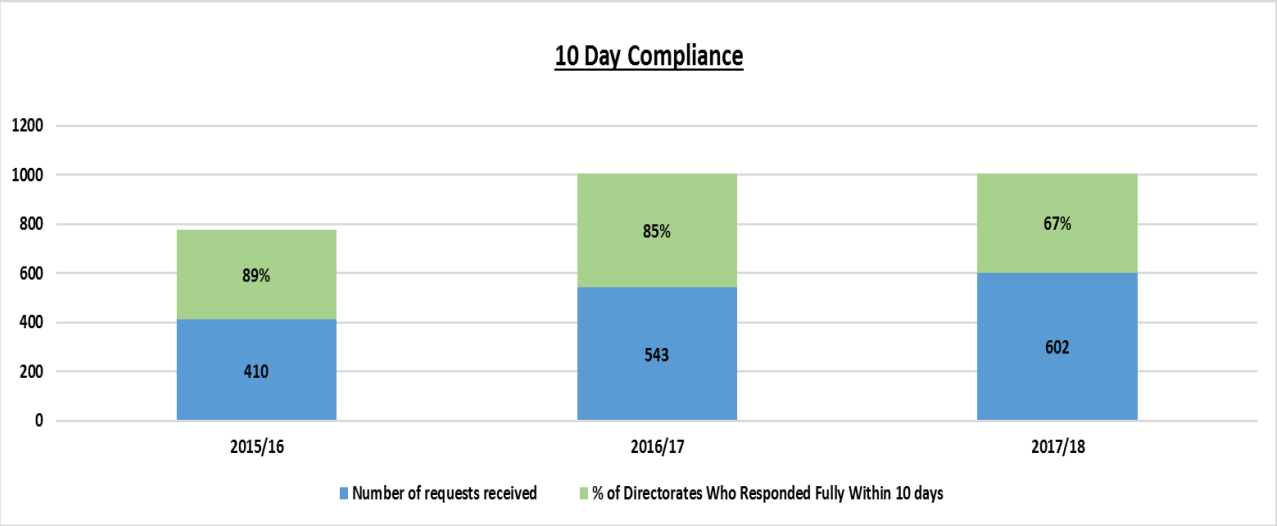
The graph below illustrates the Health Board's performance since 2012/13.



2.12.1 Performance

The FOIA team set a 10 working-day timescale to provide the required information so that the responses can be drafted and reviewed. 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. Having seen a decline in compliance over the past year we are continuing to closely monitor this.



2.12.2 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.

2.12.3 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 8 complaints about its FOIA responses in 2017/18. Of these, 1 request was sent to the Information Commissioner for further investigation.

Decision	Number
Not Upheld	2
Partly Upheld	2
Upheld	4

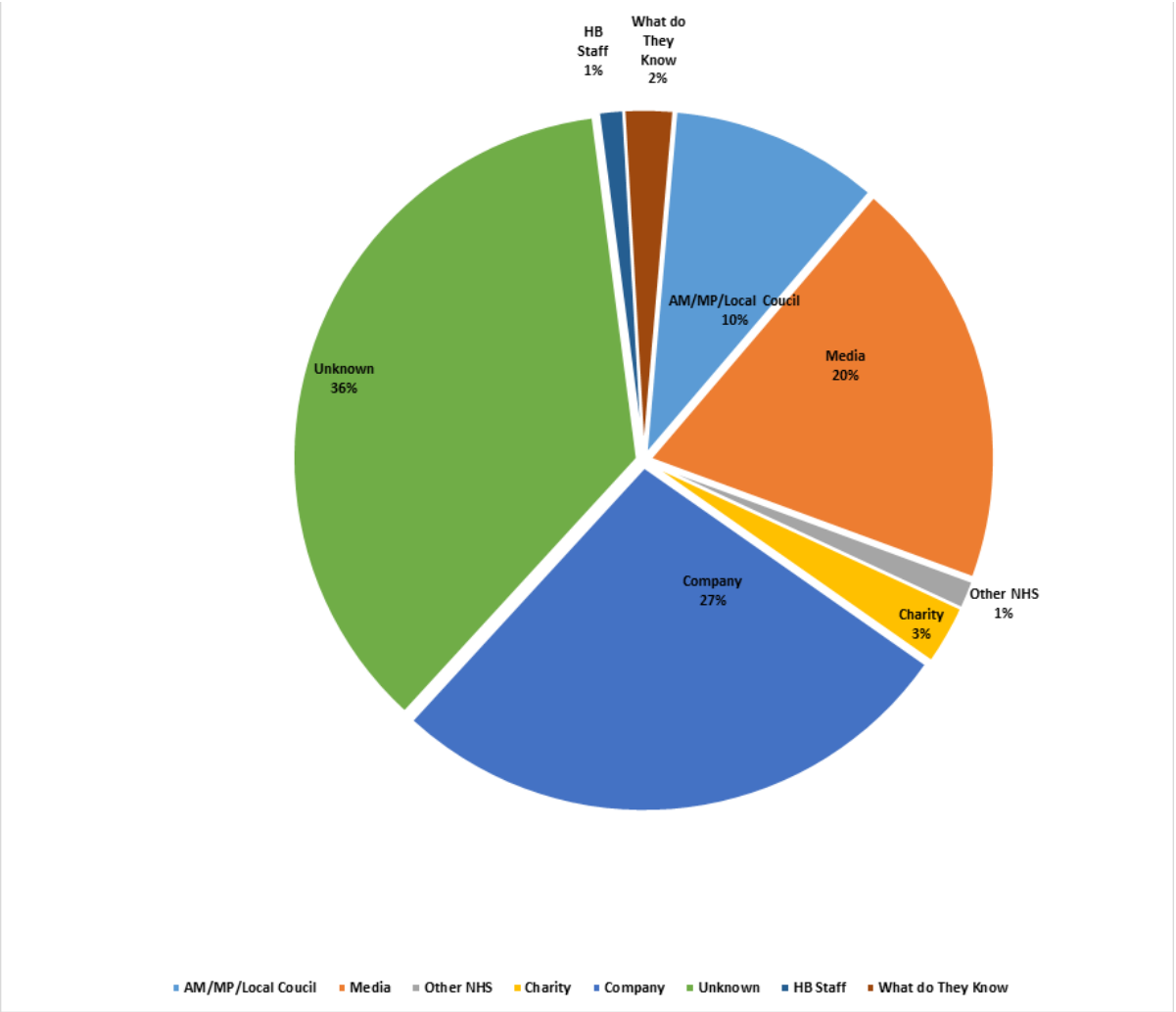
2.12.4 Request Trends and Subjects of Requests

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.)

2.12.5 Source of Requests

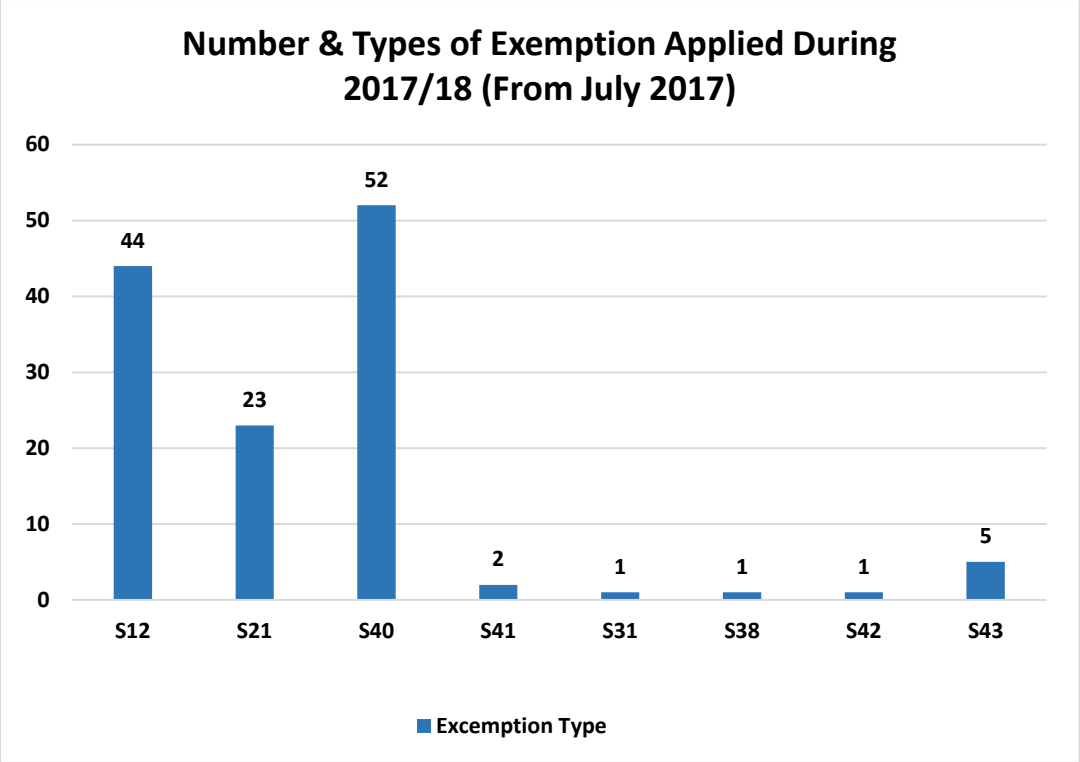
In accordance with FOIA, the Health Board maintains an 'applicant-blind' approach when providing information in response to requests. However, where that information is voluntarily provided by an applicant, the type of requester is recorded by the FOIA Team to help identify where the main demand for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

36% of all requests to the Health Board were made by sources not identified. 2% 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.



2.12.6 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 have started to record the number of requests where an exemption has been applied. Please find below the number and type of exemptions applied.



KEY:

- S12-Cost of compliance exceeds appropriate limit.
- S21-Information reasonably accessible to the applicant by other means.
- S40-Personal Information protected by the DPA / GDPR.
- S41-Information provided in confidence (but only if this would constitute an actionable breach of confidence).
- S31-Law enforcement.
- S38-Health and Safety.
- S42-Legal professional privilege.
- S43-Commercial interests.

2.13 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 priority for 2018/19 is to complete all actions on the GDPR Work Plan, and during the last phases of this plan, amalgamate outstanding actions with an updated IG Strategic Work Plan. 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.

The GDPR Work Plan was approved by IGB in December 2017. Progress is monitored bimonthly at every IGB and updates providing assurance reported to Audit Committee. The plan has taken into full consideration the requirements of GDPR, DPA 2018 and guidance issued by the ICO. There is a considerable amount of overlap with

the actions already noted on the Strategic Work Plan, and so as actions are completed on one, so they are on the other.

The GDPR Work Plan has very detailed tasks and requirements under the following IG objectives areas, which are based on the ICO 12 steps guidance to GDPR:

Objective 1 Awareness - Ensure decision makers and key people in the organisation are aware that the law is changing to the GDPR	• Continuation of communication plan utilising bulletins, intranet pages, training material, guidance documents, meetings, departmental support, promotion of GDPR requirements at all times
Objective 2 Information we hold - Document what personal data held, and with whom it is shared. Identify all of our information systems (paper and electronic)	• Continued development of the IAR will allow the IG Department to analyse the information received to better manage both the governance and also the risk associated with all information assets held • Continued work on the SharePoint site will allow much greater flexibility for the IGB Leads & identified IAOs to enter & maintain details of their information assets themselves • Continued support of the IAR User Group will help to develop best practice around the Health Board's information assets, providing assurance to IGB and the SIRO • All entries will be audited by their respective Information Asset Owners (IAOs) on an annual basis, with IG team support, to ensure the data is current, correct and to monitor the risk management process associated with each information asset • IAR will be used for assessing risk, DPIA completion, legal basis for processing, sharing agreements, access controls, retention and destruction • Links made with local and Health Board wide Risk Registers • Develop robust procedures for assessing information sharing and support of the associated required documentation • Maintain logs of all information sharing to take to IGB bimonthly • Review links between NHS and private healthcare, along with 3rd section organisations
Objective 3	

Communicating privacy information – provide people with information about our personal data collection	• A tiered approach to privacy information for patients and staff • Review existing information, promote and support new and updated notices • Link with training and IG audits
Objective 4 Individuals' Rights – Procedures must cover all rights individuals have, including deletion of personal data and to be able to provide data electronically in a commonly used format	• Develop procedures to allow accurate recording of patient preferences • Assess use of newsletters as direct marketing and review accordingly
Objective 5 Subject Access Requests (SARs)	• Develop procedures to robustly manage SARs that do not sit within a staff or patient record, e.g. emails • Manage new requirements, e.g. shortened timescales alongside no fee
Objective 6 Legal basis for processing data – Identify legal basis for processing personal data	• Ensure all information assets processed and shared have legal basis identified and formally noted
Objective 7 Consent – Controllers must be able to demonstrate consent was informed & freely given by affirmative action: Implied consent is no longer adequate	• Review consent procedures across the Health Board • Review legal basis in lieu of findings
Objective 8 Children – GDPR will bring in special protection for children's personal data	• Review privacy notices, consent and legal basis across all children's services
Objective 9 Data Breaches – Report incidents of data breach, manipulation and destruction to the supervisory authority (ICO) within 72 hours	• Finalise IG Incident Management Procedures on receipt of guidance regarding breach scoring and threshold levels for reporting to the ICO • Devise procedures for informing data subjects affected by a breach
Objective 10 Privacy by Design – Each new information system must include privacy and data protection within its specification	• Integrate DPIA findings into existing project and risk management policies • Develop an Information Risk Policy

	• Proactive approach by targeting high risk areas with DPIA information • Include DPIA information in training and IG audits
Objective 11 Data Protection Officer – For organisations that are public authorities or those that process significant quantities of personal data, a Data Protection Officer (DPO) will need to be appointed	• Ensure all relevant documentation contains DPO contact details
Objective 12 Accountability – A change in culture about responsibility & ownership: All staff to understand risks to information	• Review IG Strategy with GDPR and DPA considerations • Drive forward a significant improvement in mandatory IG training compliance across the Health Board, thereby reducing the risk of a breach, to include: - Produce a user guide for ESR based elearning - Directly support learners with elearning (a nationally updated GDPR compliant course starting May 2018) - Increase number of departmental sessions - Proactively approach poorly performing areas to engage and train staff - Encourage 'train the trainer' sessions - Produce video to be used by those without an ESR number, e.g. locums and agency staff - Liaise with Universities to ensure students on placement are trained • Significantly increase IG Audit Programme, linked to areas with poor IG training compliance, breaches, request of the IGB Lead for the area, complaints, risk assessments, walkaround findings and follow requirements of previous audits • Review all ABMU contracts, national and local, for GDPR compliance • Set up and support subgroups of IGB - Risk Management Group - IGB Leads Peer Group • Provide assurances to IGB on management of staff information as well as that of patient information • Maintain the good relationship currently held with the ICO

	• Ensure all actions completed within the ICO Audit agreed management response • Complete CPiP assessment, produce and action the corresponding Out-turn Report

SECTION 3 – CLINICAL CODING & HEALTH RECORDS

3.1 Clinical Coding Performance 2017/2018

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 2017/2018, **attaining 99%** .There were 2323 uncoded episodes at Year End out of the total of 209,636 episodes, 1.4% less than 2017/16 (212,607 episodes).

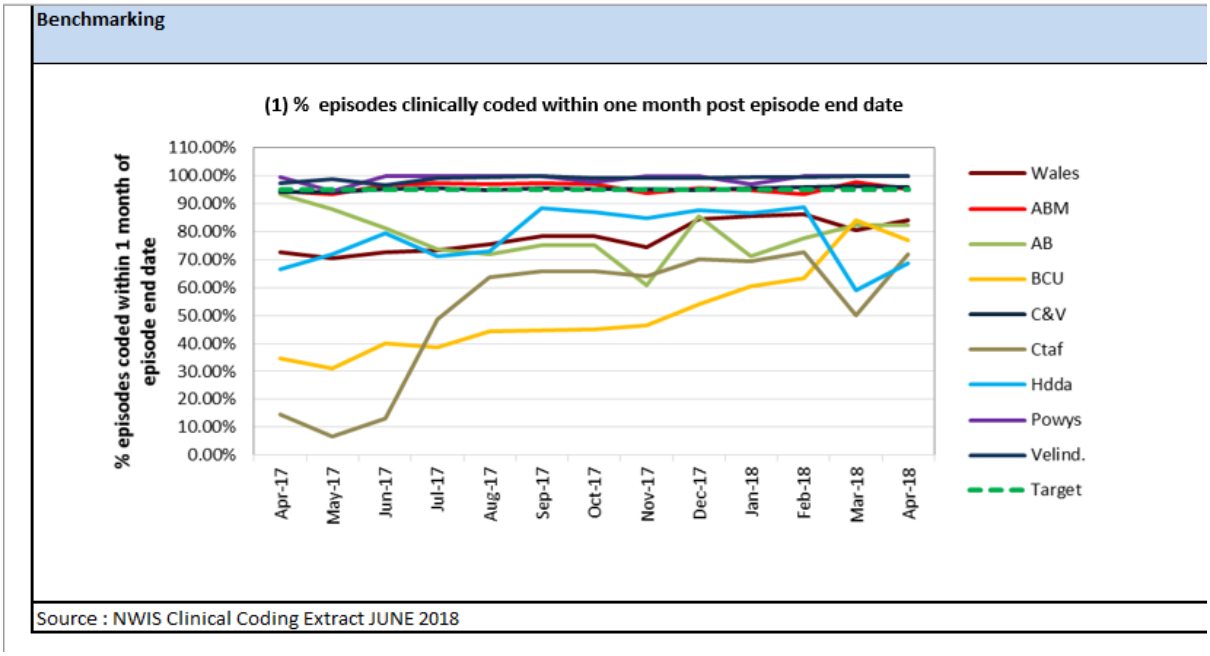
The data was submitted to NHS Wales Informatics Service (NWIS). Table 1 provides a breakdown of the 2017/2018 Year End position.

Table 1: Clinical Coding Completeness 2017/2018 - 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-17	16736	1308	92.18%	16652	103	99.38%
May-17	18074	1296	92.83%	18236	127	99.30%

Jun-17	17578	1028	94.15%	17652	117	99.34%
Jul-17	17401	873	94.98%	17467	146	99.16%
Aug-17	17296	722	95.83%	17293	165	99.05%
Sep-17	17611	644	96.25%	17369	138	99.21%
Oct-17	17611	964	95.01%	18350	154	99.16%
Nov-17	17816	2034	88.58%	17800	277	98.44%
Dec-17	16232	828	94.90%	16106	243	98.49%
Jan-18	17850	1238	93.06%	18054	296	98.36%
Feb-18	16905	1471	91.29%	16834	246	98.54%
Mar-18	17920	1307	92.71%	17823	311	98.26%
Totals				**209636**	**2323**	**99.38%**

Table 2 All Wales Clinical Coding position – demonstrates ABMU improvement and the sustained position in 2017/18



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 4.6 during 2017/18, which was higher than the previous year of 4.4.

- Signs and Symptoms coding has increased from 9.97% for 2016/17 activity to 10.2% in 2017/18, 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 2017/18 through the ongoing implementation of a detailed and robust improvement plan. During 2017/18 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 will benefit from an increasing number of staff becoming 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. 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*

3.2 Health Records

To improve the Health Records services across the Health Board for all stakeholders including Coding, the Health Records Senior Management Team has established close working relationships with Service Delivery Representatives, Information Governance Board Leads and Quality and Safety Managers to address and eradicate poor and unsafe ward administrative processes in respect of record management. The Health Records team have established from within current resources a robust audit and improvement programme to address risks and eradicate poor records management practices. Progress reports have been presented to Information Governance Board during 2017/18.

A significant development during 2017/18 has been the Health Board's success in securing Invest to Save and internal funding to initate a Health Records Modernisation Porgarmme. The programme focuses on the modernisation of the Health Records libraries. The programme will introduce a RFID solution to the clinical and logistical problems of a paper based health record and will modernise and improve the Health Records service.

The operational model will introduce RFID tagging of all acute records across all Hospital sites following a 6 month pre implementation stage. During the

implementation stage the retention and destruction team will also be recruited to maximise storage space. Further space will be required to decant non-active records and make room in Hospital libraries to introduce the location based filing model. As a result, the records library will achieve efficiency through the introduction of RFID tracking services and a retention and destruction team, realising a reduction in the Health Records establishment.

The availability of the Health Record is key to delivery safe effective care across the acute services of ABMU Health Board. Every Outpatient appoinment (600,000) and inpatient episodes (200,000) is depedent on the avaiability of the Health Record. Every clinical member of staff will enter information into the records along with all administration staff that support clinical care. There are over 3,000 known locations registered on the Welsh Patient Administration System (WPAS) where records could be located. In addition, there are 1,000's of registered holders. This demonstrates the scale and depth of the use and importance of the Health Records. Therefore, whilst the focus of the project is to modernise Health Records libraries, the impact and benefits will be experienced across the organisation.

The eventual solution to the inherent problems with the reliance on the paper clinical record is the availability of a full electronic clinical record for our patients. Successful implementation of this project will provide the Health Board with significant financial, productivity and qualitative benefits which will enhance capability to provide first class care to the population that it serves. This project will deliver a step change in the capture of clinical information and health records practices across the Health Board which is a vital first step to achieving a digitally transformed organisation.

A more detailed description of the benefits are available in Appendix S3. The Informatics Digital Strategy sets out the programme of work and vision to achieve paper-lite working in clinical areas such as, the roll-out and continual enhancement of the Welsh clinical portal to support admitted patient flow and the innovative paper-lite ways of working.

SECTION 4 – DATA QUALITY

4.1 The National Data Quality Performance Indicators

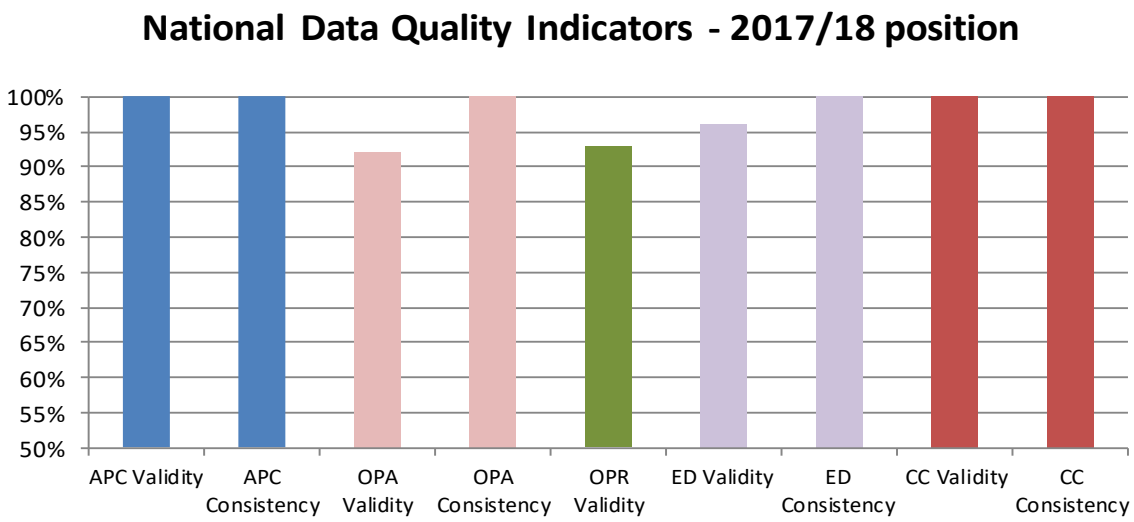
Good quality information is a fundamental requirement for the effective and prompt treatment of patients and to meet the needs of clinical governance, management information, accountability, health planning and service agreements. Poor quality data may not only affect a patient's treatment, but may also 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 2017/18 financial year is **98%**, achieving the required target for 268 of the 273 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 S4a*).



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 2017/18

The Data Quality Team has continued to support services and new developments and drive forward improvements during 2017/18, 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 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.

Full details of achievements are available in Appendix S4b

4.3 Data Quality Improvement Plan 2018/19

For the period 2018/19 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 Community Care Information System (WCCIS), Welsh Care Record Service (WCRS), Welsh Patient Administration System (WPAS), System Baseline Assessment, National Data Quality Indicators, Treatment Function Codes, Non Admitted Activity, Transgender & Adoption Process and Boundary Changes with Cwm Taf. In addition the Data Quality Kite Mark and EMPI will be progressed to further improve processes and data quality assurances.

The full description of the Data Quality Plan 2018/19 is available in Appendix S4b.

SECTION 5 – CYBER SECURITY

5.1 Key Achievements in 2017/18

Cyber Security refers to the body of technologies, processes and practices designed to protect networks, devises, 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 caused major disruption across NHS England and caused a number of patient facing services to be cancelled for a number of days. Fortunately for NHS Wales and ABMU Wannacry did not affect patient services. This was a timely reminder that Cyber Security is taken seriously and is essential for protecting services that increasingly rely on Information Technology.

5.1.1 Baseline Assessment - Stratia Report

In light of these events and building on the NHS Wales Cyber Assurance Programme, Welsh Government funded an independent review by external consults, Stratia, to carry out Cyber security assessments for the following organisations;

1. NHS Wales Informatics Service (NWIS)
2. Velindre NHS Trust (including the Welsh Blood Service) – (VCC & WBC)
3. Abertawe Bro Morgannwg University Health Board (ABMU)
4. Welsh Ambulance Service NHS Trust (WAST)
5. Aneurin Bevan University Health Board (ABHB)
6. NHS Wales Shared Services Partnership (NWSSP)
7. Cwm Taf University Health Board (CTHB)
8. Powys Teaching Health Board (PTHB)
9. Betsi Cadwaladr University Health Board (BCUHB)
10. Hywel Dda University Health Board (HDUHB)
11. Cardiff and Vale University Health Board (CVUHB)
12. Public Health Wales NHS Trust (PHW)

Following the review, each organisation received a Cyber Security assessment report and Security Improvement plan. In addition an overarching security assessment summary and security improvement plan for NHS Wales was produced.

The Stratia report assessed the Health Board against a number of known security standards namely Cyber Essentials Plus, ISO27001/2 and NIS-D the major points are listed below.

1. As part of the assessment it was highlighted that ABMU were not up to date with applying Microsoft and other software security patches. It was noted that certain traffic types (SMB) were being blocked on the network which gave a level of protection. However others were not being addressed. ABMU have worked on increasing the compliance level for servers, desktop and laptop computers and as part of an improvement initiative in this area a dashboard view was developed to give a graphical view of the patching position.

2. An area of risk identified was the use of third party software and it was clear across NHS Wales that patching of this software was of increasing concern. The ICT department considered options to address this and agreed to first consider the outcome of the national approach to Microsoft and Third Party software patching as a result of the formation of the Cyber Security task and Finish group.

3. Another area identified within the audit was the presence of old, unnecessary, unsupported software installed across the ABMU estate. This is an area that ABMU were aware of and are actively looking to employ an IT Asset Manager who will be responsible for managing the asset management software and eradicate this risk.

4. It was also pointed out that network vulnerability scans should be undertaken at least once every 6 months. These had been undertaken as part of a security programme undertaken by the Operational Security Service Management Board (OSSMB) on a yearly basis. Nationally this highlighted the following priority areas;
    a. Training and targeted phishing exercises
    b. Vulnerable Scanning
    c. Alerting software i.e. Security Information Event and Management (SIEM)
    d. A national procurement was undertaken for products to cover these areas it is anticipated that these will be implemented across NHS Wales over the next 12 months.

5. The final point raised was in connection to requirement outlined within the NIS Directive and related to the fact that data passing across local networks need to be encrypted to protect against inappropriate access and possible interception. At present locally developed web applications use the web protocol HTTP, this will now be changed to ensure that all locally developed Web applications use the secure protocol HTTPS.

Significant resources are required to identify security weaknesses, implement and manage solutions and ensure systems are monitored timely and proactively to defend against cyber security attacks. Therefore an assessment was needed to be undertaken to understand the resource requirements. As a result an additional Cyber Security role will be recruited and will be required to develop a detailed action plan for the Health Board to address areas of risk and concern in order that they are appropriately mitigated and managed.

5.1.2 NIS Directive

On 9th May 2018 UK Government implemented new controls on the security of Network and Information Systems (NISD) of essential service providers, the NHS being one of these providers. The reason for this directive is to ensure there is a national framework to support and promote the security of networks and information systems, consisting of a National Cyber Security Strategy, a computer security incident response team, a single point of contact and a national NIS competent authority. The competent authority for NHS Wales is Welsh Government. This directive will be audited by the competent authority and failing to implement the specified controls may result in a fine up to a maximum of £17million. Whilst this has been adopted into UK Law the detail is still being worked on and is different to the GDPR data protection regulation.

Although this directive came into legislation in May 2018 and the 14 objective areas have been defined the competent authority (Welsh Government) are still to make public the threshold expected for these areas. It is expected that these will be made available at the end of June 2018 following this a full gap analysis and action plan will be developed.

5.1.3 Infrastructure Improvements

During 2017/18 a number of network infrastructure replacements were undertaken to ensure non supported and obsolete equipment was replaced. Part of this work was the replacement of end of life network switches at both Morriston and Singleton Hospitals.

A major project was undertaken across Singleton , Maesteg, Tonna and Angelton (at Glanrhyd) Hospitals, following Welsh Government funding for enabling wireless. Wi-Fi is available at these sites for accessing information at the point of care and providing free Wi- for staff, visitors and patients within those sites to bring them up to the same level as the other acute hospitals. The Wi-Fi network is not only utilised by computers and laptops, a number of medical devices now connect via this technology. To support this a new dedicated Wi-Fi service set identifier (SSID) has been implemented, which allows the medical data to be separated from non-medical data in order to protect the data and minimise the risk of cyber-attack across both types of equipment.

As part of the prevention work undertaken, the Health Board firewalls were configured to monitor all data travelling through them to identify a possible cyber-attack. This software was configured in monitor mode during 2017 and early 2018 to give a visibility of any potential risks, it is planned that this will be escalated to blocking mode during 2018. This is essential to make full use of the firewall defence system but needs to be implemented in a way that will cause the least amount of disruption. Other areas of work undertaken were;

- Further security in the way of encryption has been added to network switches.
- Assessment to secure access to the Local Network and mitigate against a user plugging in an unauthorised device onto the network which may introduce virus/malware or be used to export data from the network. Costs to be identified.
- Assessing tighter controls on medical devices and the Internet of things (ioT) devices.

Nationally two products have been procured by NWIS on behalf of NHS Wales to provide better analysis of activity across its network, these products are a Security Information Event Management (SIEM) software and Network Vulnerability assessment software. Both these products will be centrally managed but will also require local installations and IT resources. The SIEM will collect information in the form of logs from local devices, which will be constantly fed back to the central assessment engine where they will be analysed and interrogated to see if there are any unusual or possibly malicious activity taking place. The SIEM has already been implemented within NWIS on a number of important National infrastructure devices. The second product, the network vulnerability assessment, will allow the Health Board to meet the requirements of the Stratia report and analyse its network on a regular timescale and highlight areas where security software may need to be strengthened.

Asset Management is another identified priority following an audit which was carried out by shared services internal audit. The Health Board has gone through a process of engaging with one of its major suppliers to undertake a baseline assessment of its Software licence position. Following this assessment the department has been fine tuning the asset system SNOW which has helped to understand the infrastructure assets better (hardware and software). This work has highlighted the need for a dedicated Asset Manager post who will be responsible for progressing the 3 year improvement plan. The recruitment process has started and it is hoped to have this position filled by the end of the summer 2018.

5.1.4 Review of Vulnerable Infrastructure

During 2017/18 significant progress was made in identifying and replacing obsolete operating systems on desktop and laptops

- Window XP Cymru domain connect devices have all been removed. The final device was removed in April 2018.
- Windows 7 reaches end of live in January 2020. A plan to upgrade all devices to Windows 10 is in place. Rollout of Windows 10 devices commenced in May 2017 with 2200 Windows 10 PCs/Laptops already migrated.
- Microsoft Office 2007 reached end of live in October 2017. The migration to Office 2016 is ongoing. To date there are 6000 Office 2016 completed with the remaining 3,800 devices to be migrated by the end of August 2018.
- Imprivata Single Sign on has been implemented in the A&E departments at Morriston and NPT Hospitals. The Imprivata solution uses fast user switching and an RFID card to tap on a reader to provide access based on the user's credentials and therefore systems are fully auditable. This solution is key moving forward to reduce the amount of generic logins which were historically implemented to reduce login times.
- Windows Server 2003 instances - 97 Windows 2003 servers in place with a target date for removal of December 2019.

5.1.5 Service Catalogue Development

The IT Service Catalogue offers a way to:

- Document and publish the specific range of available services
- Standardise service deliverables
- Establish service level expectations
- Determine associated costs of service and supports contract management

It is a means by which IT services can be defined, configured, deployed and governed. When used effectively, a Service Catalogue is an excellent communication tool, and a highly effective resource in the invent of a cyber-security attack, providing a complete up to date picture of the IT estate and supports decision making on priorities and risks. ABMU started the implementation of the service catalogue in February 2016 with the development of a SharePoint site. 257 services are now identified in the Service Catalogue.

5.2 Development of the strategy, capability, resources and operational priorities 2018/19

The growing threat posed by Cyber Security requires a coordinated and sophisticated approach. To achieve this ABMU will be working with partners and NWIS to develop a robust approach and strategy, prioirtise for 2018/19 are as follows

5.2.1 Strategy Development

Key activity for 2018/19 will be the implementation of the Startia report recommendations and action plan. The progress against the actions will be reported

to the Information Governance Board and Service Management Board. The implementation plan will seek to address the gaps found as detailed above.

5.2.2 Patching

Without a robust plan and resources to ensure high standards of operational management in relation to patching activity, there is a significant risk that future Cyber Security threats will infect ABMU and NHS Wales, resulting in ICT service disruption and associated clinical, financial and reputational impacts. The server inventory has been categorised into the following groups:

- Fully automatic updates
- Automatic Deployment with Manual reboot
- Manual only
- 3rd party supplier responsibility (but monitored)

Servers marked as fully automatic are patched with all available patches on a two week basis. A dashboard presents server status against available patches from the update server, servers needing a reboot and days since last reboot. Currently the service is achieving between 90-93% compliancy. Desktop and laptops patching is managed through WSUS patch manager and is currently patching all devices connected to the network, this gives an overall compliance figure of over 96% as certain devices are not always connected to the network. There is a plan to move away from WSUS and to perform patching through SCCM, this is being planned to be implemented early in financial year 2018/19.

The current patching baseline and updates on progress will be reported to the service management board (SMB). It is expected that this information will be provided in the form of a dashboard with risk escalated to the risk register.

One other area that can cause significant problems is the possibility of username and password details being compromised and these details used to gain access to information they should not have. To combat this Microsoft LAPS has recently been implemented across the Health Board which means that any configuration changes and software installs now have to be given a one time password to allow this to take place. Alongside this work the IT Department will be removing accounts that have elevated rights to reduce the risks highlighted above.

5.2.3 Anti-virus (AV)

The dashboard developed last year will continue to be rolled out across the department and gives visibility the levels of compliance for desktops. In 2018/19 the department will actively be monitoring its position with regard to Anti Virus software as the Health Board has Kaspersky Anti Virus installed and some concerns have been expressed across the UK that the software may be used to facilitate cyber attack from

Russia. The advice given by the NCSC is that currently this software is safe to use and this position will be continually monitored.

5.2.4 Firewall

In 2017/18 firewall rules were strengthened in line with national requirements and installed software that assesses all traffic that is passed through the firewalls to identify any adverse activity. This software has been running in 'monitor mode' in 18/19 the full block mode will be enabled to strengthen cyber security defenses.

5.2.5 Non-IT Managed Devices

As part of the plan developed to look at the protection levels on the Health Board network the work to evaluate a number of products, which assess the traffic on the network and alert the IT Department of any irregular activity will continue in 2018/19. This will build on the proof of concept that has already been undertaken with one supplier. During July and August 2018, two further products will be assessed. The evaluation will deliver a product that will have a sophisticated solution to block malicious activity and inform the IT Department of risks. Following a successful proof of concept it is planned that a full business case is produced for the procurement and management of this system. If this business case is then successful it is hoped that this can be implemented late 2018 to early 2019.

5.2.6 Asset Management

A significant amount of work has been undertaken on asset management of IT equipment over the past year and asset management software has been fully rolled out across the organisation. To support this an in-house workflow management system has also been developed and implemented. The whole asset management system was recently audited by internal audit which has highlighted areas where further work needs to be undertaken. To this end it has been approved that a dedicated Asset manager will be appointed who will be responsible for implementing the 3 year plan. The department is currently advertising for this post.

5.2.7 Incident Management and Backup and Recovery

An Informatics incident response and business continuity plan is being developed and is planned to be submitted to the senior team for approval. 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.

5.2.8 ABMU Staff

A training package to raise awareness of cyber security has been procured by NHS Wales and the Health Board is planned to be implementing during 2018/19, this will be rolled out across the Health Board. A resource plan for the cyber security team will be developed to ensure appropriate systems, monitoring and user training is in place to deliver safe and secure systems for the Health Board. Elements of this will also be

considered by the All Wales Cyber Security Task and Finish Group to ensure consistency.

Appendix

S3 – Appendix Clinical Coding and Health Records

S3 Appendix Clinical Coding and

S4 – Data Quality

S4 Appendix - Data Quality.docx