Copy of Status Report to Health Board January 2018 on General Data Protection Regulations

ABM University Health Board	
23rd January 2018 Audit Committee **Agenda item:2b**	
	STATUS REPORT – GENERAL DATA PROTECTION REGULATION
Prepared by	Sian Richards, Head of Digital Records and Information Assurance
Approved by	Matthew John, Assistant Director of Informatics Hamish Laing, Executive Medical Director
Presented by	Hamish Laing, Executive Medical Director. Senior Information Risk Owner (SIRO)

1. Purpose

The Director General for Health and Social Services and Chief Executive of **NHS Wales wrote to all Health Boards in October 2017 to set out the impact of The General Data Protection Regulation** (**GDPR) on the NHS in Wales and set the expectation that Organisation were actively preparing for its implementation. The letter stated that GDPR would be an agenda item at future** NHS Wales Executive Board Meeting so that progress of all Health Boards' readiness and compliance could be reviewed.

May 2018 will also see the introduction of the **Network and Information Systems (NIS) Directive.** The NIS Directive is aimed at bolstering cyber security across sectors that rely heavily on information and communications technology, including Health Boards in Wales.

This report advises the Health Board on ABMU's current readiness for the introduction of GDPR and the NIS Directive.

2. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) come into force on 25th May 2018 and will be directly applicable as law in the UK. It will replace the Directive that is the basis for the UK Data Protection Act 1998. Although in general the principles of data protection remain similar, there is greater focus on evidence-based compliance with specified requirements for transparency, introduces a principle of 'accountability' and more extensive rights for data subjects and considerably harsher penalties for non-compliance up to 4% of turnover per breach.

The GDPR introduces a principle of *'accountability'*. This legally 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 **within 72 hours** of knowledge of the breach occurring, and for the investigation to be fully completed and reported upon with a few weeks

- The appointment of a suitably qualified and experienced Data Protection Officer

- Under the GDPR, the fines available are significantly increased to 4% of turnover, and may be imposed **for *any* infringement** of the Regulation, not just data security breaches.

Whilst the GDPR represents an evolution of Data Protection law there is still a considerable amount of work required to meet the basic standards and compliance with the Regulation. In November 2017, in preparation for GDPR, all NHS Organisations in Wales were asked to produce a Readiness Statement to be considered by the Wales Information Governance Board (WIGB). WIGB provides assurance to Welsh Government about the privacy and sharing of information across Wales and includes, as a member, the Deputy Director of Digital Health and Care at Welsh Government. The position statement was a national template, based on Information Commissioner's Office (ICO) guidance of how organisations should prepare for GDPR. The return clearly shows that based on current resources and readiness, ABMU **will not be compliant with the law from May 2018**.

A summary of ABMU's ability to meet legal requirements by May 2018 is shown below:

1. Awareness	Green = On target Yellow = Currently off target but deliverable at the expense of all non-GDPR IG Departmental work Red = Off target
2. Information and Assets held	
3. Communicating privacy information	
4. Individuals' rights	
5. Subject Access Requests	
6. Lawful basis for processing personal data	
7. Consent – review of current models	
8. Children – Review of information and conset processes	
9. Data breaches – investigation and mitigations	
10. Data Protection Impact Assessments	
11. Data Protection Officers	
12. International Operations	

A comparison across Wales with figures available at this time is shown below:

Organisation	Compliant	On target	Currently off target but deliverable	Off target
BCU	1	11	0	0
Cwm Taf	2	10	0	0
NWSSP	3	9	0	0
PHW	1	9	2	0
Velindre	1	9	2	0
NWIS	0	6	6	0
WAST	0	6	6	0
Aneurin Bevan	0	6	6	0
Hywel Dda	0	4	6	2
Cardiff		2	6	4
ABMU	**0**	**2**	**4**	**6**

A more detailed assessment has been carried out locally in preparation for GDPR, based on the themes identified in the all Wales assessment, to produce an ABMU specific action plan. This is summarised **by the current status of readiness**:

33 tasks	Off target
4 tasks	Currently off target but deliverable
20 tasks	On target
0	Compliant
57 tasks	**TOTAL**

Non-achievement of the plan is a consequence of the resources available to the IG team and has been identified by Welsh Audit Office in their feedback that, based on current resources, ABMU will **not be compliant with GDPR when it comes into force in May 2018**.

The IG Department has to deliver all IG training to the organisation, manage high profile breaches and lead the organisation towards improved IG practices. This resource deficit has reported previously to IGB and Audit Committee, and was placed on the Corporate Risk Register in March 2017. Now, with the added General Data Protection Regulations assurance cannot be provided to the Health Board that we will meet all our requirements under the law.

As a result of non-compliance ABMU faces the likelihood of a significant financial penalty from the ICO. Under GDPR, the ICO may impose fines up to at **4% of turnover** per breach or area of legislative non-compliance. The ICO have advised the Health Board recently that if there are further breaches or general IG standards and training compliance are not improved upon, their response to a breach would be less lenient in the future. Under GDPR, it is not only mandatory to report all notifiable IG breaches, but also that general non-compliance is sufficient for a fine to be levied, irrespective of whether or not there has been a breach. Specific failures in ABMU that may result in a fine include:

- Poor IG training compliance. ABMU have had official notice that training compliance requires improvement
- Inability of the Organisation to investigate and report IG breaches within the legal timeframe (72 hours)
- Lack of a robust IG audit programme
- Lack of risk management and mitigation
- Lack of Privacy Impact Assessments
- Lack of adequate fair processing notices for patients and staff (transparency regarding information management and sharing)

- Lack of a robust process for managing information sharing

The IG Department is prioritising work according to Organisational need alongside some 'quick wins'. The team are utilising the operational support of unit IGB Leads and the Information Security Manager wherever possible to extend the resources available. Following the IGB in December the preparations for GDPR will also be added as a significant risk to the Organisation.

To mitigate the risk and improve the readiness of the Health Board for GDPR, in December 2017 the Executive Team approved an approach to address the shortfall in resource. A business case is now being developed for approval by the Investment and Benefits Group (IBG) in January 2018 for a substantive increase in resources for the IG team. The approach also included advance approval for temporary additional support to provide immediate support and to improve compliance and reduced risk to the organisation. Increasing the resources will improve ABMUs readiness position and could bring it line with other Health Boards in Wales. Under GDPR there is an ongoing need to maintain standards, the work required is not a one off exercise. The resources will also provide the ability to maintain the standards and compliance recurrently and ensure a continued GDPR compliance to mitigate against penalties and poor IG practices.

3. The Network and Information Systems (NIS) Directive

The Network and Information Systems (NIS) Directive was adopted by the European Parliament on 6th July 2016. Member States have until 9th May 2018 to transpose the Directive into domestic legislation. The NIS Directive is aimed at bolstering cyber security across sectors that rely heavily on information and communications technology. Certain businesses operating in critical industries are known as Operators of Essential Services (OESs). OESs are public or private entities that meet all of the following criteria:

- The operator provides a service that is essential to society and the economy.
- The service rendered depends on network and information systems.
- An incident to the network and information systems of that service would have significant effects on its provision.

The NIS Directive impacts on the following services:

- Energy;
- Transport;
- Water;
- Banking;
- Financial market infrastructures;
- Healthcare; and
- Digital infrastructure.

The directive therefore will apply to Health Boards and Trusts in Wales and ABMU Informatics are working closely with Welsh Government (WG), NWIS and other Health Board/Trust Leads to finalise the reporting and implementation plans. As the Competent Authority, WG are gathering relevant information from Health Boards/Trusts and by March will produce incident thresholds as to what needs to be reported against *e.g.* a computer failure that leads to loss of healthcare to a 1000 people, or disruption to a hospital servicing 10,000 people.

Ownership of risk belongs to the OES rather than the Competent Authority. The onus will be on the Health Board to demonstrate to WG that appropriate measures are being applied to manage the risks to networks and information systems that fall within the set thresholds.

In parallel to the preparations for the NIS Directive, ABMU continue to focus on cyber security as a top priority. Since the Wannacry virus attacked computer systems worldwide in May 2017, ABMU Informatics

have made several improvements across patch management, firewalls and anti-virus monitoring. ABMU have collaborated with NWIS and other Health Boards/Trusts to prioritise the capital monies allocated to NHS Wales cyber security and to commission a NHS Wales Cyber Security Assessment by an external cyber security consultancy. ABMU were one of the first organisations to undergo the assessment in November and has received a draft report which reflects the significant progress made since Wannacry and further recommendations for improvement. Once the report is finalised, the recommendations and associated resource requirements will inform our preparation for the NIS Directive.

Financial penalties for non-compliance of the NIS Directive are likely to be the same as GDPR and organisations can be fined simultaneously under both legislations. A full impact assessment of the NIS Directive will be prepared for Information Governance Board (IGB) in January 2018 and issues escalated as required.

4. Recommendations

The Health Board to note the significance of both the GDPR and the NIS Directive which come into force in May 2018.

The Health Board to note that ABMU do not expect to be compliant with the GDPR based on current resources, and plans are being put in place to secure additional investment to improve the position.

The Health Board to note the progress being made with regards to cyber security and the workload and resource implications of the NIS Directive and recommendations from the National Cyber Security Assessment.