General Data Protection Regulations (GDPR)

Final Internal Audit Report

2018/19

Cwm Taf University Health Board

September 2018

NHS Wales Shared Services Partnership

Audit and Assurance Services

Contents **Page**

Review reference:	CTU-1819-18
Report status:	Final
Fieldwork commencement:	1 June 2018
Fieldwork completion:	5 July 2018
Draft report issued:	1 August 2018
Management response received:	14 August 2018
Final report issued:	20 August 2018
Auditor:	Martyn Lewis
Executive sign off:	Robert Williams, Director of Corporate Services and Governance / Board Secretary
Distribution:	Gwenan Roberts, Head of Corporate Services Claire Northwell-Todd, Information Governance
Committee:	Audit Committee

ACKNOWLEDGEMENT

NHS Wales Audit & Assurance Services would like to acknowledge the time and co-operation given by management and staff during the course of this review.

Disclaimer notice - Please note:

This audit report has been prepared for internal use only. Audit & Assurance Services reports are prepared, in accordance with the Internal Audit Charter and the Annual Plan, approved by the Audit Committee.

Audit reports are prepared by the staff of the NHS Wales Shared Services Partnership – Audit and Assurance Services, and addressed to Independent Members or officers including those designated as Accountable Officer. They are prepared for the sole use of Cwm Taf University Health Board and no responsibility is taken by the Audit and Assurance Services Internal Auditors to any director or officer in their individual capacity, or to any third party.

1. Introduction and Background

A review of the arrangements in place to consider Cwm Taf University Health Board (the 'Health Board' or the 'organisation') preparedness for the introduction of the General Data Protection Regulation within the Health Board has been completed in line with the 2018/19 Internal Audit Plan.

The General Data Protection Regulation (GDPR) was adopted on 27 April 2016. It took effect from 25 May 2018 and was immediately enforceable as law in all member states of the European Union (EU).

The primary objectives of the new legal framework are to institute citizens' rights in controlling their personal data and to simplify the regulatory environment through a unified regulation within the EU. Many principles of the GDPR are broadly the same as the existing Data Protection Act (DPA). However, one of the most significant changes is the increased penalties. Under the new regulations, penalties will reach an upper limit of €20m or 4% of annual turnover, whichever is higher.

In October 2017, Stratia Consulting was commissioned by Velindre NHS Trust on behalf of NHS Wales, to carry out external cyber security assessments for its organisations. The review included an assessment against the GDPR requirements included in the IASME standard. The IASME Governance standard is based on international best practice, is risk-based, and includes aspects such as physical security, staff awareness, and data backup. The IASME governance self-assessment includes the cyber essentials assessment within it, as well as an assessment against the requirements of the GDPR.

For each organisation, including the Health Board, a cyber-security assessment report and security improvement plan (SIP) was produced. Additionally, an overarching security assessment and SIP for NHS Wales as a whole was produced.

The relevant lead for the assignment is the Director of Corporate Services and Governance.

2. Scope and Objectives

The overall objective of the audit was to provide assurance to the Health Board that arrangements are in place and managed appropriately within its wards, departments and directorates to ensure compliance with the requirements of the GDPR.

The areas the review sought to provide assurance on were:

- appropriate action is being taken to ensure that management and staff are aware of the GDPR and the impact it is likely to have;
- local governance controls and measures have been implemented to enable compliance with the GDPR; and
- a register of information assets is maintained and identifies the source, responsibility and sharing arrangements for each asset.

The review also draws on the findings of the GDPR aspect of the cyber-security review carried out by Stratia Consulting to ensure that appropriate actions have been undertaken to rectify any identified weaknesses in the Health Boards preparation for GDPR.

3. Associated Risks

The potential risks considered in the review were as follows:

- insufficient preparation for the new GDPR resulting in non-compliance with the requirements of the regulation;
- controls not operating resulting in non-compliance with GDPR; and
- reputational damage and/or financial loss.

OPINION AND KEY FINDINGS

4. Overall Assurance Opinion

We are required to provide an opinion as to the adequacy and effectiveness of the system of internal control under review. The opinion is based on the work performed as set out in the scope and objectives within this report. An overall assurance rating is provided describing the effectiveness of the system of internal control in place to manage the identified risks associated with the objectives covered in this review.

The level of assurance given as to the effectiveness of the system of internal control in place to manage the risks associated with GDPR is **Reasonable** assurance.

RATING	INDICATOR	DEFINITION
Reasonable assurance		The Board can take **reasonable assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. Some matters require management attention in control design or compliance with **low to moderate impact on residual risk** exposure until resolved.

The Health Board has undertaken a great deal of work to prepare for GDPR to enable compliance. Guidance has been produced and disseminated via the Information Governance team, and procedures have been revised. The Health Board has set up a process for developing its Information Asset Register (IAR) which is underway, and guidance for this process has been provided to staff.

Our testing identified some issues, in particular, not all departments have pushed awareness of GDPR within their area.

The Health Board uses REDCap (an application for building and managing surveys and databases) to create its IAR. This process allows for the capture of risk information and identification of basis for processing and information flows. However, we note that the IAR is a work in progress and our testing identified that although there are over 500 entries, many of these do not have the risk assessment section completed. In addition, not all departments that we looked at had made entries onto the IAR. Furthermore, there are some inconsistencies in the approach taken between departments.

We did not identify any findings that we would consider to be high priority during our audit fieldwork.

The overall level of assurance that can be assigned to a review is dependent on the severity of the findings as applied against the specific review objectives and should therefore be considered in that context.

5. Assurance Summary

The summary of assurance given against the individual objectives is described in the table below:

Assurance Summary					
1	Appropriate action is being taken to ensure that management and staff are aware of the GDPR and the impact it is likely to have.				✓
2	Local governance controls and measures have been implemented to enable compliance with the GDPR.			✓	
3	A register of information assets is maintained and identifies the source, responsibility and sharing arrangements for each asset.			✓	

** The above ratings are not necessarily given equal weighting when generating the audit opinion.*

Design of Systems/Controls

Our findings from the review have highlighted one issue that would be classified as a weakness in the system control/design for GDPR.

Operation of System/Controls

Our findings from the review have highlighted seven issues that are classified as weaknesses in the operation of the designed system/control for GDPR.

6. Summary of Audit Findings

In this section we highlight areas of good practice that we identified during our review. We also summarise the medium priority findings made during our audit fieldwork. The detailed findings are reported in the Management Action Plan (Appendix A).

Appropriate action is being taken to ensure that management and staff are aware of the GDPR and the impact it is likely to have.

We note the following areas of good practice:

- there is a formal group with an Independent Board member who oversee Information Governance and who were overseeing the preparation for GDPR;
- there was good central coordination and effort to ensure the Health Board complies with GDPR;
- the level of compliance with the information governance module in ESR eLearning has increased across the Health Board;
- the Information Governance team have provided a good amount of guidance and undertaken appropriate awareness raising actions in preparation for GDPR;
- there is an information governance work plan to enable GDPR compliance;
- there was an GDPR preparation plan with all items that we looked at being progressed appropriately;
- the Information Governance Group (and the GDPR task and finish group) monitors progress against actions identified to enable compliance with the GDPR; and
- all relevant items of the Stratia report regarding GDPR have been addressed.

We did not identify any medium priority findings in relation to this objective.

Local governance controls and measures have been implemented to enable compliance with the GDPR.

We note the following areas of good practice:

- the departments that have identified 'subject access requests' as their biggest GDPR risk have revised their procedures to deal with this;

- some departments have set up a process to monitor and track access requests to ensure compliance;
- work has been undertaken within most departments to raise awareness and processes have been changed to enable compliance with the GDPR;
- posters from the information governance team have been put up within many departments to raise staff awareness of GDPR;
- most departments are aware of the Privacy Impact Assessment (PIA) process and have undertaken this where relevant;
- some departments are using the IAR process to rationalise their information assets, validate the basis for them, and to ensure that unneeded records are removed;
- the R&D directorate have utilised training and information provided on national basis that is specific to R&D;
- the work of the R&D directorate is monitored by the R&D Committee, with GDPR being included on the agenda;
- the Health Research Authority (HRA) has provided updated wording for consent and provision of information for patients; and
- the HRA has provided new agreements for cross border research where agreements explicitly state that all parties must comply with GDPR.

We note the following medium priority finding:

- there has been no significant work done to raise awareness and ensure compliance with GDPR within the Head and Neck directorate. This is exacerbated by the low compliance rate for the directorate with the Information Governance Mandatory Training module (at 52%).

A register of information assets is maintained and identifies the source, responsibility and sharing arrangements for each asset.

We note the following areas of good practice:

- there is an IAR in place for GDPR with a process for all departments to feed in their information;
- the GDPR page on the intranet contains guidance on how to complete the IAR;
- as at the end of June 2018 there were over 500 entries on the IAR, which demonstrates that the processes are operating across the Health Board;
- the IAR process captures the basis for processing and information flows;
- many departments have requested that all staff identify assets for inclusion; and

- a review of a sample of assets indicated that information was correct within the IAR.

We note the following medium priority findings:

- although there are currently over 500 items on the IAR the majority of entries do not have the risk section completed. In addition, there appears to be a degree of confusion within departments over how to record some information assets, and we note inconsistencies in recording assets on the IAR; and
- not all departments have started entering items onto the IAR, with neither R&D or Head and Neck directorate creating entries.

7. Summary of Recommendations

The audit findings, recommendations are detailed in Appendix A together with the management action plan and implementation timetable.

A summary of these recommendations by priority are outlined below.

Priority	H	M	L	Total
Number of recommendations	**0**	**3**	**5**	**8**

Finding 1 – IAR process (Operating effectiveness)	Risk
Although there are currently over 500 items on the IAR the majority of entries do not have the risk section completed. This section requires an assessment of the risk presented by the data by factoring the source and flow of the data alongside storage and the basis for processing. Without this risk assessment there is no consideration of information flows, or the basis for processing for many of the assets contained on the IAR. In order to progress to the risk assessment section, the initial section has to be signed-off by the Information Governance team. However, the limited resources available in the team means that this process is delayed. In addition, we understand that there is a degree of confusion within departments over how to record some information assets on the IAR, and inconsistencies in recording approach. For example: • Not all departments have recorded staff files that are held within the department, with the assumption being that they are covered by HR's registration. • Some departments have registered network folders in entirety, and some have registered individual records held on the network.	Controls not operating resulting in non-compliance with GDPR

Recommendation	Priority level
The guidance on completing the IAR should be reiterated to all departments, with key points highlighted. Management should consider providing 'carved out' time within the Information Governance team to focus on the IAR.	**Medium**
Management Response	**Responsible Officer/ Deadline**
There has been a delay in completing the action plan due to the available resource within the team. The second phase of the risk management section has been issued to all of the Information Asset Owners. Reminders are sent to directorates have not yet responded, but delays are inevitable with completion especially in clinical areas. The IAR has only recently been rolled out so a vast amount of work has been undertaken and completed in a short time. In relation to confusion, a guide is available on the SharePoint site and has been circulated to IAR owners. Networks and individual folders will be on the register – this would occur where access levels are different or the information held is different. Where there are different criteria, this may cause disparity in the way they are recorded. Directorates will again be reminded of the importance of keeping the IAR up to date and we will also raise awareness of common areas such as staff record management.	Claire Northwell-Todd September 2018 for further reminders

Finding 2 IAR completeness (Operating effectiveness)	Risk
While many departments have started to create their IAR, at the time of our fieldwork not all departments had started entering items onto the IAR, with neither the R&D or Head and Neck directorate creating entries.	Controls not operating resulting in non-compliance with GDPR.
Recommendation	**Priority level**
All departments should be reminded to complete the IAR.	**Medium**
Management Response	**Responsible Officer/ Deadline**
As stated, the IAR has only recently been rolled out. We concentrated on phase one initially, with the second stage of the risk assessment section only commencing in May. GDPR legislation is the beginning of implementing change in process as opposed to the deadline. Reminders have been issued to departments.	Claire Northwell-Todd September 2018 for further reminders

Finding 3 Directorate work (Operating effectiveness)	Risk
There has been no significant work done to raise awareness and ensure compliance with GDPR within the Head and Neck directorate. Furthermore, it appears that this matter may be exacerbated by the low compliance rate with the Information Governance Mandatory Training module (at 52%). However, we acknowledge that the risk of non-compliance with GDPR is partially mitigated by the type of area it is, as clinical staff are professionally used to maintaining patient confidentiality.	Insufficient preparation for the new GDPR resulting in non-compliance with the requirements of the regulation
Recommendation	**Priority level**
All departments should be asked to confirm that GDPR is included within governance meetings and that awareness is raised.	**Medium**
Management Response	**Responsible Officer/ Deadline**
We have raised this issue with the Directorate Manager for Head and Neck, and the Lead within the Chief Operating Officers team. We have raised the issue of compliance with the training modules and reminders will be sent to staff.	Neil Cooper September 2018

Finding 4 Access requests resources (Operating effectiveness)	Risk
The introduction of GDPR has amended the requirements for providing data subjects access to their data, in particular the timescale has reduced to 1 month, and there is no longer the ability to charge for the access. Although staff and departments that we spoke with were aware of the revised requirements for subject access requirements within GDPR, the resource in place for dealing with these within departments has not been increased. Should GDPR result in a significant increase in requests, (with anecdotal evidence indicating that this is the case) then the Health Board may not be able to comply without additional focussed resource.	Controls not operating resulting in non-compliance with GDPR.
Recommendation	**Priority level**
The Health Board should monitor the level of access requests and include the risk on the appropriate risk registers. Additional resource should be provided in the event of non-compliance.	**Low**
Management Response	**Responsible Officer/ Deadline**
The Health Board continues to routinely monitor the subject access process for various directorates via the key performance indicators report presented to the Information Governance Group on a quarterly basis. The report includes number of requests received (by month) and the number that breach the legal timescales.	Claire Northwell-Todd December 2018

Finding 5 R&D (Operating effectiveness)	Risk
R&D were not part of the Health Board's GDPR group, as a separate R&D group was set up with HCRW (Healthcare Research Wales). However, due to national work undertaken for R&D, the remit of this group was unclear and there were no meetings. As such, there was no visibility of R&D on any GDPR planning meetings within the Health Board which has contributed to a lack of awareness within R&D of the Health Board's processes relating to the following elements of GDPR: • privacy notices; • privacy impact assessments; and • subject access requests.	Controls not operating resulting in non-compliance with GDPR.
Recommendation	**Priority level**
R&D should fully engage with the Health Board's processes and procedures regarding GDPR.	**Low**
Management Response	**Responsible Officer/ Deadline**
R&D have been made aware of the Health Board processes and procedures. A member of the Academic Partnership Board was also on the group. The Information Governance Officer is a member of the Research Group so will pick up any issues via this method.	Claire Northwell-Todd /Prof John Geen December 2018

Finding 6 Posters (Operating effectiveness)	Risk
The Health Board has developed 'raising awareness' posters and 'staff privacy' notices to raise awareness of GDPR. However, during our fieldwork we noticed that not all departments had placed the poster or notice on notice boards.	Controls not operating resulting in non-compliance with GDPR.
Recommendation	**Priority level**
Posters / information should be displayed on boards.	**Low**
Management Response	**Responsible Officer/ Deadline**
We will send a further reminder to directorates of the requirements. Information materials are available via the SharePoint site. The privacy information has been sent to directorate managers / senior managers for escalation. Staff are signposted to this information at the induction sessions, and at the monthly classroom sessions. The e-learning package also asks employees to familiarise themselves with the intranet and the IG page specifically.	Claire Northwell-Todd October 2018

Finding 7 IAR monitoring (Operating effectiveness)	Risk
There is no functionality within REDCap (an application for building and managing surveys and databases) to identify departments that have not entered any information assets on the register, and no process to monitor this within the Information Governance team. As such, the process is very reliant on departments themselves to record information on the IAR.	Controls not operating resulting in non-compliance with GDPR.
Recommendation	**Priority level**
An assessment of the departments included on the IAR should be undertaken to identify those who have not completed the IAR exercise. As part of this a timetable for all departments to have submitted entries should be set out.	**Low**
Management Response	**Responsible Officer/ Deadline**
This is difficult to collate due to the way that the REDCap system is set up. However, the IG team will export into excel and filter to review potential gaps.	Claire Northwell-Todd December 2018

Finding 8 Departmental Actions (Operating effectiveness)	Risk
As part of our work we noted good practice in some departments that were not always replicated in all departments: • work has not always been undertaken within departments to raise awareness and processes have not always been changed to enable compliance with the GDPR; • not all departments have set up a process to monitor and track access requests to ensure compliance; • posters from the information governance team have not always been put up within departments to raise staff awareness of GDPR; and • some departments are using the IAR process to rationalise their information assets, validate the basis for them, and to ensure that unneeded records are removed, however not all departments are doing this.	Controls not operating resulting in non-compliance with GDPR.
Recommendation	**Priority level**
These items of good practice should be shared across the Health Board.	**Low**

Management Response	Responsible Officer/ Deadline
Discussions will be held with the two directorates identified to establish how they record and process access requests. The posters issue will be picked up when audits of departments are reinstated. The material is available electronically but should be displayed in public facing areas.	Claire Northwell-Todd January 2019

Appendix B - Assurance opinion and action plan risk rating

Audit Assurance Ratings

 **Substantial assurance** - The Board can take **substantial assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. Few matters require attention and are compliance or advisory in nature with **low impact on residual risk** exposure.

 **Reasonable assurance** - The Board can take **reasonable assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. Some matters require management attention in control design or compliance with low to **moderate impact on residual risk** exposure until resolved.

 **Limited assurance -** The Board can take **limited assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. More significant matters require management attention with **moderate impact on residual risk** exposure until resolved.

 **No assurance** - The Board can take **no assurance** that arrangements to secure governance, risk management and internal control, within those areas under review, are suitably designed and applied effectively. More significant matters require management attention with **high impact on residual risk** exposure until resolved.

Prioritisation of Recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows.

Priority Level	Explanation	Management action
High	Poor key control design OR widespread non-compliance with key controls. PLUS Significant risk to achievement of a system objective OR evidence present of material loss, error or misstatement.	Immediate*
Medium	Minor weakness in control design OR limited non-compliance with established controls. PLUS Some risk to achievement of a system objective.	Within One Month*
Low	Potential to enhance system design to improve efficiency or effectiveness of controls. These are generally issues of good practice for management consideration.	Within Three Months*

* Unless a more appropriate timescale is identified/agreed at the assignment.