The Shrewsbury and Telford Hospital NHS Trust

Paper 6

Recommendation ☑ **DECISION**	The Board is asked to make a decision on implementing a new role of Data Protection Officer as mandated by the General Data Protection Regulations (GDPR) and the Information Commissioner (ICO) to ensure and monitor compliance with the new GDPR requirements and be accountable to the Board.
Reporting to:	**Trust Board**
Date	8th February 2018
Paper Title	Compliance with the new General Data Protection Regulations (GDPR)
Brief Description	GDPR is an EU regulation that will come into force on 25th May 2018. It is recommended that all Board members are aware of forthcoming changes to the law and potential changes in information security standards. GDPR will be the responsibility for the whole Board, including Non-Executive Directors to provide assurance that the law is complied with. There are many changes related to 'data processing' that will impact on both employees and service users (Data Subjects).
Sponsoring Director	Neil Nisbet, Finance Director / Senior Risk Owner (SIRO)
Author(s)	John Cliffe, Chief Information Officer and Jill Stretton IG Manager
Recommended / escalated by	
Previously considered by	Sustainability Committee 28th November 2017
Link to strategic objectives	VALUES IN PRACTICE – Value our workforce to achieve cultural change by putting our values into practice to make our organisation a great place to work with an appropriately skilled fullly staffed workforce.
Link to Board Assurance Framework	If we do not get good levels of staff engagement to get a culture of continuous improvement then staff morale & patient outcomes may not improve (RR 423)
Outline of public/patient involvement	The GDPR involves all British Citizens
Equality Impact Assessment	◉ **Stage 1 only (no negative impacts identified)**
Freedom of Information Act (2000) status	◉ **This document is for full publication**

The Shrewsbury and Telford Hospital NHS Trust

Paper 6

EXECUTIVE SUMMARY

1. Recommendations

The Board are asked to note the main changes required of the General Data Protection Regulation (GDPR) and the financial (resource) impact on the organisation and to consider the appointment of a Data Protection Officer.

2. Introduction

The GDPR is an EU regulation that will come into force on 25th May 2018. Many of the main themes within GDPR are the same as the current Data Protection Act and therefore will provide a starting point for the Trust to progress towards compliance with the new requirements of GDPR.

The organisation will have to do adopt a different approach to data management within the new landscape of Data Protection within the UK. Therefore, it is vitally important the Trust begins to consider GDPR in all aspects of current business function and the changing landscape as it emerges across the Health Economy. Failure to implement these changes effectively could have a detrimental effect to the organisation post 25th May 2018.

GDPR introduces greater accountability for all organisations. All Board members need to be aware of forthcoming changes to the law and potential for change in information security standards. GDPR will be the responsibility for the whole Board, including Non-Executive Directors to provide assurance that the law is complied with. The main changes are:

- Appoint a Data Protection Officer (DPO)
- Implementation of appropriate technical and organisational measures to ensure the Trust complies with GDPR. This will include internal data protection policies, staff training, internal audits of processing activities and reviews of internal HR policies.
- Maintain a register of all incidents of data sharing
- Implement measures that meet the principles of Data Protection By Design including:
    - Data Minimisation for data sets and data collection;
    - Pseudonymisation when sharing information to a greater level than we currently do including producing randomised information;
    - Transparency with regards to what we are doing with data;
    - Allowing individuals to monitor the processing of their data – staff and patients now have strengthened rights to;
        - Be informed what is happening with their data
        - Access their information free of charge and in a format that is accessible to them (there will be no cost recovery from access to records after the 25th of May 2018)
        - Alter their records if they believe something is incorrect
        - Erase their records at their request
        - Restrict processing down to individual level or stop the Trust processing their data completely on request

- Transfer data to an organisation of their choice in an appropriate method to the individual
- Object to their data being processed in a specific way – i.e. research, statistics, direct marketing, profiling, performance of a task in the public interest
- Refuse for their data to be used in an automated decision making process.

- Creating and improving security features on an on-going basis

- Use Data Protection Impact Assessments in the use of new technologies or a change in the management of data, monitoring and CCTV.

The GDPR is continuing to evolve as the guidance is still being developed by the Information Governance Alliance and the Information Commissioner's Office.

Appointing a DPO as mandated by the GDPR, is essential to achieving effective facilitation across the organisation. The organisation must ensure that the DPO has proven expert knowledge of data protection law and practices, and the ability to perform the tasks specified in the GDPR.

3. Options

It is important to consider EU guidelines that '*the DPO cannot hold a position within an organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.'* The role of the DPO may be shared by multiple organisations that are 'public authorities' taking into account organisational structure and size, and may be either a member of staff or may fulfil the task on the basis of a service contract, provided there is no conflict of interest.

4. Impact Analysis

Resource impact on current IG processes

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 (ICO).

5. Proposal(s)

Appointment of a Data Protection Officer whose job description is compliant with GDPR requirements e.g.:

- The DPO reports to the highest management level e.g. Board level.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

6. Risks & Mitigations

In terms of Regulation and Enforcement

- Enact additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.
- Allow the Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4% of global turnover for the most serious breaches.

7. Implementation Plan

As a health organisation we need to consider the development and implementation of action plans to achieve this demonstrable compliance. Areas to be addressed include:

- Revision of IG and related policies and statutory reporting requirements
- Assessment and allocation of resources needed to support the DPO role
- Information asset registers and maps of information flows
- Provide full disclosure on the use and sharing of personal data and the legal basis
- Review of contracts to ensure compliance
- Revision of subject access procedures to reflect new timescales and removal of charges
- Development of or revision of procedures to address data subjects' rights that are established by the GDPR.

This list of actions is not exhaustive

8. Conclusion

The Board are asked to note the resource impact of the GDPR and the Data Protection Bill 2017 requirements and consider the appointment of a Data Protection Officer.