Sherwood Forest Hospitals
NHS Foundation Trust

Board of Directors - Public

Subject:	General Data Protection Regulation (GDPR)	**Date:** 31st August 2017	
Prepared By:	Shirley A Clarke, Head of Corporate Affairs and Company Secretary		
Approved By:	Shirley A Clarke, Head of Corporate Affairs and Company Secretary		
Presented By:	Shirley A Clarke, Head of Corporate Affairs and Company Secretary		
Purpose			
To provide assurance to the Board with regard to the organisations preparedness for the implementation of the new GDPR from May 2018		**Decision**	
		Approval	
		Assurance	x

Strategic Objectives				
To provide outstanding care to our patients	**To support each other to do a great job**	**To inspire excellence**	**To get the most from our resources**	**To play a leading role in transforming health and care services**
x	**x**	**x**	**x**	**x**

Overall Level of Assurance				
	Significant	**Sufficient**	**Limited**	**None**
		x		

Risks/Issues	
Financial	The Trust could incur significant financial penalties if it breaches the regulations
Patient Impact	Sharing of patient data may be restricted under the new regulations
Staff Impact	Staff must be fully informed in order to ensure the regulations are implemented across the Trust
Services	
Reputational	**Publicised breaches of the regulation could have a negative reputational impact**

Committees/groups where this item has been presented before

N/A

Executive Summary

The GDPR, which was approved in 2016 and comes into force on 25th May 2018, will be directly applicable as law in the UK.

The GDPR introduces a principle of 'accountability' which requires organisations to be able to demonstrate compliance with the regulations.

There are 12 areas of focus:

- Awareness
- Information you hold
- Privacy Notices
- Individuals' Rights
- Subject Access Requests (access to records)
- Lawful Basis for Processing Personal Information
- Consent
- Children
- Data Breaches

- Privacy by Design and Data Protection Impact Assessments
- International

A detailed action plan has been developed and a Compliance Group established.

The Board will receive regular updates with regard to progress via the Audit and Assurance Committee report.

General Data Protection Regulation (GDPR)

The GDPR, which was approved in 2016 and comes into force on 25th May 2018, 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 It will replace the Directive that is the basis for the UK Data Protection Act 1998, which will be repealed or amended.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.

In general, the principle of data protection remain similar; however 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 key changes which will take effect under GDPR are listed in brief below.

Change	**Impact**
Awareness	Data Controllers should make sure that decision makers and key people in the organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have. Regular updates through committee and SIRO reporting.
Information you hold	Data Controllers must maintain internal records of processing activities. They must document what personal data is held, where it came from and who it is shared it with. An information audit across the organisation or within particular business areas to identify the data processed and how it flows into, through and out of the organisation, is recommended
Privacy Notices	When personal data is collected the current requirement is to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR organisations must explain their lawful basis for processing the data and how long it will be retained.
Individuals' Rights	On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements.
Subject Access Requests (access to records)	Information must be provided at no charge, with tighter timeframes to comply with requests.
Lawful Basis for Processing Personal Information	A lawful basis must be identified for all data processing activities involving personal and sensitive personal information.
Consent	Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and organisations will need to provide simple ways for people to withdraw consent.
Children	The GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If organisations' offer online services ('information society services') to children and relies on consent to collect information about them, then they may need a parent or guardian's consent in order to process their personal data lawfully.

Change	Impact
Data Breaches	The 72-hour requirement for reporting serious data breaches will be mandatory across all sectors. Financial penalties may be up to 4% of organisations' worldwide turnover (current limit is £500,000).
Privacy by Design and Data Protection Impact Assessments	Undertaking Data Privacy Impact Assessments where processing is likely to pose a high risk to individuals' rights and freedoms and incorporating data protection measures by default in the design and operation of information systems and processes.
Data Protection Officers	The appointment of a suitably qualified and experienced Data Protection Officer that must report directly to the highest management level of the organisation.
International	Cross-border processing agreements will require determination of the supervisory authority – whether this is ICO or equivalent authority in other countries.

The GDPR introduces a principle of 'accountability' which requires organisations to be able to demonstrate compliance with the regulations.

In order to ensure achievement, a detailed action plan, segmented into the 12 key areas has been developed; all actions have been allocated an owner and timeline. A Compliance Group has been established which comprises of clinical representation from each division and corporate representation from NHIS, Procurement and Governance Support Unit. The Information Governance Manager has overall responsibility for the delivery of the plan.

The Information Governance group will provide oversight of the plan and report directly to Audit and Assurance committee who will update the Board on progress, through the committee reporting process.