msb group
Mid Essex Hospital Services NHS Trust
Southend University Hospital NHS Foundation Trust
Basildon and Thurrock University Hospitals NHS Foundation Trust

Meeting Title	Trust Boards in Common		
Date	9th May 2018	**Agenda item**	13
Report Title	European Union General Data Protection Regulation Implementation Update		
Lead Director/ Manager	Martin Callingham, Chief Information Officer & Senior Information Risk Owner		
Report Author	Matt Barker, Group Head of Information Governance		
Freedom of Information (FOI) Status	Unrestricted		
Action Required*	Approval □ Decision □ Discussion □ Information ☑ Other (specify) □		
Executive Summary	This paper provides an update of the current position regarding meeting compliance with the new General Data Protection Regulation and highlights key potential associated risks and issues.		
Recommendation	To note the content of the Report and the actions being taken in preparation for GDPR		
Trust Strategic Objectives	Objective 1 – Deliver high quality care whenever needed		
CQC Key Lines of Enquiry	KLoE W6.7: Are there robust arrangements (including appropriate internal and external validation) to ensure the availability, integrity and confidentiality of identifiable data, records and data management systems, in line with data security standards? Are lessons learned when there are data security breaches?		
NHS Constitution	Principle 3- The NHS aspires to the highest standards of professionalism and excellence.		
Implications			
Risk	**Potential Financial Risk:** The new General Data Protection Regulation will substantially increase the monetary fine for any breach of the Regulation - including serious Information Governance breaches - from the current £500,000 to 4% of annual turnover, or €20m whichever is the greater.		
Legal	Nil		
Resources	Nil		
Previously Considered by	None		
Appendices			

General Data Protection Regulation (GDPR) Implementation Update

Introduction and Overview:

The General Data Protection Regulation comes in to effect on 25 May 2018 and replaces the current Data Protection Act 1998. The aim of the regulation is to give greater transparency about personal citizen data (digital and paper) that is held and used both public and private companies across the European Union.

GDPR will be an ongoing programme of work as each new development or data capture has to be assessed against the regulation. The NHS has a long history of managing sensitive and confidential patient data and the new regulations do not represent a significant change for staff. It does however require changes to the way we document and record the way we, and companies that work with the MSB group, hold and manage patient data.

The new regulations apply to all of Europe. Guidance on how the NHS will interpret and implement the regulations has been slow to be issued. Specific NHS guidance for the implementation of GDPR was not issued by the Information Governance Alliance until late February 2018. A raft of further guidance remains unpublished (including: Privacy by design and default, Personal data breaches and notification, GDPR overview, Transparency and subjects' rights). This is scheduled for release in May.

An action plan has been put in place which is based on guidance issued in the Information Governance Alliance (Department of Health IG) "The General Data Protection Regulation: Implementation Checklist" (IGA, February 2018) and RSM Internal Audit Recommendations from BTUH and MEHT. This action plan is being implemented across the 3 sites simultaneously and utilising the same templates, tools and policies.

This paper provides an update of the current position of the Group in relation to GDPR implementation, including assurances and the key issues/risks.

Current Position:

There has been a considerable amount of work on preparing the Group for GDPR, with positive engagement from operational staff and leadership teams. A brief overview of some of the key areas that are on target to be delivered by 25 May are outlined below:

- Information Governance policies and procedures across the 3 trusts have been reviewed in line with the new regulation and are being finalised. Wherever possible the documents have been amalgamated so there is one policy/procedure document across the 3 sites (i.e. An Information Governance Policy & Framework, Information Security Policy, Information Sharing). These will be presented at Group Document Control on 16 May and published shortly after.

- GDPR compliant Privacy Notices are being drafted in line with guidance issued by the Information Commissioner's Office and Information Governance Alliance, and following review of the limited returns from the Data Flow Mapping Exercise (which is ongoing). These will be circulated to relevant areas for public display and published on Trust websites and staff intranet in good time prior to 25 May.

- Mandatory Information Governance Training for staff is being revised to reflect the new regulation and will be published prior to 25 May, utilising current local IG training packages. Going forward, there will be standardised IG training package across the Group with the Personnel & Organisational Development team offering assistance to implement this.

- Information Governance breach reporting mechanisms are already established across the Group to report all Level 2 serious IG breaches to the Information Commissioner's Office via the NHS Digital incident reporting tool. The Information Governance Alliance and NHS D is reviewing the current reporting mechanisms and will be releasing new guidance shortly. In the meantime, confirmation has been received from NHS Digital to continue using the existing method of breach reporting until further notice.

- Privacy Impact Assessment and Information Sharing Agreement templates have been revised to take the new regulation in to account and are already in use across the organisation. The Privacy Impact Assessment templates are part of the Digital Services Project Brief Document issued at the commencement of a new project.

- A Data Flow Mapping exercise was issued in early 2018 to ascertain personal data flows into and out of the 3 Trusts. This piece of work informs the Information Governance function of any risks, data sharing agreements that need to be put in place, and identifies any areas where a Privacy Notice is required (the legal basis for processing personal data). This piece of work is ongoing and is highlighted in the GDPR Key Risks and Issues section below.

- Information Asset Registers have been circulated across the Group to identify Information Asset Owners and the mechanisms/systems in place to ensure the organisation understands what information it holds, who is responsible for the information, the legal status of the information, and how it can legally be used. This is on going and highlighted in the GDPR Key Risks and Issues section of this paper.

- The mandatory position of Data Protection Officer required under new GDPR has been appointed by the Joint Executive Group in January 2018.

GDPR Key Risks and Issues:

There are a number of areas that have been highlighted as being a potential risk to the Group requiring further action to take forward:

	Narrative	Risk	Mitigation/Resourcing Requirements
Information Asset Register – a list of all systems that hold and use patient data	A register has been a prerequisite of the annual Information Governance Toolkit assessment for a number of years and therefore should be in place across the 3 trusts. The Information Asset Register (IAR) document was sent to Information Asset Owners/Administrators (System Managers) across the Group in February 2018.	There is a risk that staff do not understand their accountability for patient data held on these systems and unintended breaches could occur.	Ownership of systems is through the identification of an Information asset owner who has responsibility to ensure that data is held safely A process has commenced and is ongoing to actively engage with operational teams to establish Information Asset ownership by 25 May. Local and corporate responsibility has been documented. IG managers are meeting with areas to identify owners. Trust managing directors are supporting the process to ensure all systems have appropriate ownership.
Data Flow Mapping - Understanding were, how and why patient data is stored	The template for the Data Flow Mapping exercise was cascaded to all relevant department leads across the Group in February 2018. The Information Governance function provided support to complete this task.	There is a risk that areas across the group will not understand or know about small areas of data held by parts of the service.	A process has commenced and is ongoing to actively engage with operational teams to establish data flows by 25 May. This process links closely with the identification of the IAO. Some areas have not identified asset ownership and there for not all data mapping is complete. Escalation processes to Managing Directors has been agreed.
Review of Contracts with third parties that process data	Under the GDPR, there is a requirement to have a written contract in place between the organisation and the third party processing personal data. This is important so the parties understand their responsibilities and liabilities.	There is a risk that contracts with third party providers/suppliers that process personal data on behalf of the Group will not have been reviewed/amended as required under the appropriate articles of GDPR.	Companies are being contacted using the standard Crown commercial service contract variation issued in April. Companies are being contacted on a priority basis. Due to the number of companies that contract with the MSB group there is a risk that this process may to continue past May 25th however the remaining companies will be low risk.

			All new contracts with the MSB use the standard NHS terms of conditions and are covered by GDPR. Companies that work with the group work under these terms of conditions and privacy impact assessments are also completed.
Policies and procedures	Under the GDPR, there is a requirement for all policies and procedures relevant to data processing to be compliant. This is important so that staff are aware and understand their responsibilities.	There is a risk that current policies and procedures relevant to data processing will not be compliant with GDPR.	Polices and procedures have been identified and are being updated and will do through the document management committee on 16th Education of changes will continue following sign off.