Ashford and St. Peter's Hospitals NHS Foundation Trust

TRUST BOARD
31 May 2018

AGENDA ITEM NUMBER	16.3	
TITLE OF PAPER	General Data Protection Regulation (GDPR) Update for Trust Board	
Confidential	YES	
Suitable for public access	NO	
PLEASE DETAIL BELOW THE OTHER SUB-COMMITTEE(S), MEETINGS THIS PAPER HAS BEEN VIEWED		
STRATEGIC OBJECTIVE(S):		
Best outcomes		Compliance with GDPR
Excellent experience		
Skilled & motivated teams		
Top productivity		
EXECUTIVE SUMMARY		
	The General Data Protection Regulation (GDPR) comes into force on 25 May 2018 and will be directly applicable to UK law. The Trust has been closely following guidance provided by the Information Governance Alliance (IGA) and the Information Commissioner's Office (ICO), and is also working closely with IG teams in our neighbouring trusts. The IGA has provided guidance to focus on 12 key areas, which the Trust has used as the basis for an action plan, with several key tasks completed or underway. Other actions require clearer interpretation of the legislation; more guidance is expected from the central teams.	
RECOMMENDATION:	Receive and obtain assurance	
SPECIFIC ISSUES CHECKLIST:		
Quality and safety		
Patient impact	Patients will be informed and assured of how we process their data.	
Employee	Staff will be informed and assured of how we process their data.	
Other stakeholder		
Equality & diversity		

Finance	
Legal	We have a legal requirement to comply.
Link to Board Assurance Framework Principle Risk	
AUTHOR(s)	Jane Townsend, Information Governance Manager Laura Ellis-Philip, Associate Director of Informatics
PRESENTED BY	Simon Marshall, Director of Finance and Information
DATE	25 May 2018
BOARD ACTION	The Board is asked to note the report.

General Data Protection Regulation (GDPR) Update for Trust Board

Introduction

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018 and will be directly applicable to UK law. The new Data Protection Bill 2018 (DPA18). also received Royal assent in May. Both the GDPR and DPA18 will need to be viewed side by side to ensure compliance with data protection legislation. Upon leaving the EU, GDPR will not be directly applicable in the UK but compliance with the DPA18 will ensure continuity as the same principles apply.

GDPR applies to all data controllers and processors within the EU. The GDPR will apply to the Trust as data controller, where we determine the purposes and means for processing personal data of both employees and patients, and also as data processor, where we are responsible for processing personal data on behalf of another data controller. The GDPR represents a change in the way that data is protected and managed, and introduces new rights for data subjects. In addition, it strengthens and expands existing rights available under DPA 1998, and the new Data Protection Bill 2018.

The Trust has been closely following guidance provided by the Information Governance Alliance (IGA) and the Information Commissioner's Office (ICO), and is also working closely with IG teams in our neighbouring trusts. The IGA has provided guidance to focus on 12 key areas, which are detailed below.

As the legislation becomes clearer, more guidance is expected.

Key requirements of the GDPR as advised by the IGA

1. Awareness and Accountability - While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR raises their significance. Accountability as a Data Controller is not only required but the Trust must be able to demonstrate compliance. Currently under DPA98 data controllers provide certain information under fair processing and privacy notices that cover processing activity. With DPA18 and GDPR more specific and extensive detailed information is required about how all personal data is processed and the legal basis to do so in each case.

The new Data Protection and Security Toolkit, which replaces the IG Toolkit, gives good guidance on the evidence the Trust needs to comply with this element.

2. Information you hold - The Trust is required to fully document the personal data it holds, where it came from, who it is shared with and the legal basis under which it is used/shared.

The Trust has an Information Asset register where we will store this information.

3. Communicating Privacy information - The right to be told is perhaps the right that is most strongly enhanced, as this requirement means that more information will need to be routinely provided to patients (via patient leaflets and privacy notices) detailing the legal basis for processing their data, how the Trust will use information, retention periods and who we share this information with for all processing activities. Through such notices the Trust is required to detail what 'rights' the patient has and how to exercise them.

The Trust is currently in the process of generating all the required privacy notices and is working with front line services to tailor their service specific notices.

4. Individuals' rights - GDPR enhances Data Protection rights for individuals which will affect the way the Trust manages information. This is likely to result in essential changes to operational systems relating to:

- the right to object to certain types of processing being undertaken (to stop personal data being used for certain purposes such as marketing)
- the right to restrict processing (to stop personal data being used)
- the right to data rectification (to have personal data changed if inaccurate)
- changes to the way data subjects can request their information under subject access (including less time to respond to requests and understanding what processing is carried out on their data)
- the right to data portability (allows individuals to obtain and reuse their personal data for their own purpose and for it to be moved, copied or transferred easily from one IT environment to another in a safe and secure way, without hindrance to usability).
- the new right to erasure (allows patients to have their records deleted in rare circumstances) Some rights to erasure will already exist within the Trust, for example, where data continues to be held post-employment and where no ongoing legal relationship exists or where data is collected for membership purposes.

The full impact of this factor has been considered with the main outstanding issue under consideration being around the use of .

5. Subject access requests (SARs) - Under DPA98, individuals have the right to obtain copies of information held about them by organisations. The timescale for complying with a request has reduced from 40 calendar days to one month. In addition, the Trust was previously able to charge a fee of £10 per request, however, under GDPR no fee will be payable by the applicant.

The Subject Access Team process these requests. They have stopped charging and are working to new deadlines. They will report on any significant impact as it comes to light.

6. Legal basis for processing personal data - Article 30 makes it mandatory for organisations to record all of their processing activities. Records of information processing are already being collected using the Trust information asset register. However, further work needs to be undertaken to ensure that a full account of the Trust's processing activities are recorded. This is necessary due to the change in emphasis concerning liability for data loss. Previously, data controllers assumed full responsibility for the conduct of their data processors and needed to ensure that they had undertaken adequate due diligence before entering into a contractual relationship.

The GDPR at Article 28 section 4 has shifted the emphasis so that if a processor engages a third party processor to undertake work they assume the responsibility for any liability/loss emanating from that extended contractual relationship. Crown Commercial Services published a GDPR Policy note on the 19th December 2017 setting out how public bodies should apply the upcoming changes in data protection law to existing and prospective contracts. The contractual terms of all data controllers in common and data processors will need to be reviewed. The new 2017/19 NHS Standard Contracts have now been updated (May 2018) and are available.

This is one of the more complex aspects and needs consideration. Further advice and guidelines from the IGA are expected.

7. Consent - GDPR sets a very high standard for consent to process data. Organisations must ensure consent is clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. Existing processing is under review to identify either if there is a requirement for written consent or if there is another legal basis for processing to rely on. Where consent is used as the legal basis to process personal information (normally for secondary, non-care purposes), this needs to be freely given, specific, informed, unambiguous, and only processed for the direct

purpose it was obtained. Consent cannot be assumed, inferred from silence, or by pre-populated tick boxes. The main premise of the GDPR is that individuals are fully informed about how their data is processed, that processing is legitimate and that consent for processing can be revoked.

With regard to direct patient care, the Trust can rely on Article 6 (1) (e) of the GDPR which relates to the processing of information for health and concerns the processing of data for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This means that the legal basis for collecting data in this instance will not be by the patient giving their consent.

With regard to staff, Article 6 (1) (b) states that where processing of data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This section is applicable to staff recruitment and the processing of data for the furtherance of that employment.

Privacy Notices for both staff and patients have been developed and published. They have been issued to key groups such as Members and other distribution lists we hold.

8. Children – organisations should consider putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity. Gillick competence will still apply.

The Trust will develop a privacy statement which can be easily understood by children.

9. Data Breaches - Where individuals are likely to suffer some form of damage or risk to their rights and/or freedoms as a result of a breach, there will be a requirement to notify the ICO within 72 hours. It will also be mandatory to report high risk breaches directly to the data subject(s). Failure to report may result in a fine, as well as a fine for the breach itself.

GDPR allows the ICO to impose significant fines for data breaches. The maximum fine available is currently £500,000 but this will rise to €20 million, or 4% of annual turnover per breach.

The Trust already has procedures in place within the IG team to notify the ICO in a timely manner when a breach is brought to their attention. A publicity campaign to ensure this message is understood by all staff will be launched shortly.

10. Data Protection by design and privacy impact assessments – Data Protection Impact Assessments will be routinely required for all new projects, ensuring that privacy and data protection is considered in the early stages when; building/purchasing new IT systems, sharing data with other organisations, using data for new purposes.

The Trust already performs Privacy Impact Assessments for all new IT projects that come through the Informatics department. Other departments will be required to follow this process.

11. Data Protection Officer – All public authorities must appoint a statutory Data Protection Officer. This is a dedicated senior level role which monitors Trust compliance with data protection. The DPO must report directly to the highest level of management (to a member of the Trust board).

The Trust Board has appointed the Information Governance Manager as the DPO, reporting in to the Director of Finance and Information via the Associate Director of Informatics. The lines of communication are good.

12. International – all organisations operating internationally should determine which data protection supervisory authority they come under.

Action Plan Update
A GDPR action plan has been developed to address the main areas of work that are required to ensure compliance with GDPR. Work is underway and several points have already been addressed. For example, Privacy Notices have been developed and published. It is important to note that as an NHS organisation the Trust already has good governance in place as part of the evidence developed each year for the Information Governance Toolkit, and as such is in a much stronger position than many private companies who are facing these stricter guidelines for the first time.

The IG Manager has been meeting with departments such as Contracts, Procurement, Comms and HR who will be directly affected by the new legislation to explain the impact of the law.

The Trust has its own bespoke information asset register which has been in place for many years and is kept up to date. This will be further developed to incorporate the data privacy impact assessment process and the legal bases for all information processing activity, mandatory for all data processing under the new legislation.

Conclusion
The Trust continues to work on strengthening and refining our systems to meet the GDPR requirements as well as on communicating everything it means for staff and patients. Further clarity on the interpretation of some of the requirements is needed so that we can clearly identify all actions we need to take as a Trust. The resource of the IG function is under consideration in order to support a smooth implementation of the regulations as well as maintaining future compliance.

An action plan is in place to ensure that the Trust understands and fulfills its obligations under GDPR/DPA

The Board is asked to note the report.