Oxford University Hospitals
NHS Foundation Trust

Trust Board Meeting in Public: Wednesday 17 January 2018

TB2018.18

Title	**Progress report regarding organisational preparedness for the General Data Protection Regulation (Data Protection Act 2018)**

Status	For assurance
History	Ad-hoc

Board Lead(s)	Peter Knight, Chief Information & Digital Officer			
Key purpose	Strategy	**Assurance**	Policy	Performance

Executive Summary

1. The General Data Protection Regulation/Data Protection Regulation 2018 will have legal effect from the 25th May 2018.
2. To ensure preparedness the Trust IG department has undertaken a GAP analysis and produced an action plan to ensure that the Trust is compliant with the changes in legislation.
3. It is anticipated that the Trust will be compliant with the new legislation. The only area of potentially foreseeable risk is ensuring that all contracts with data controllers in-common and data processors are compliant with the new legislation

Progress report regarding organisational preparedness for the General Data Protection Regulation (Data Protection Act 2018)

Introduction

1. This paper provides an overview of work being undertaken by the Information Governance (IG) department to ensure organisational preparedness for the advent of the General Data Protection Regulation (GDPR)/Data Protection Act (DPA) 2018.

2. The GDPR/DPA 2018 will become legally enforceable in the United Kingdom (UK) on the 25th May 2018. European Union (EU) regulations have directly applicable legal status for all EU member states. Notwithstanding the UK referendum decision to leave the EU, the UK will still be obliged to comply with this Regulation. However, the Regulation does not encompass all legal obligations and provides member states with the opportunity to make some modification to how the legislation will be applied within the new DPA 2018. Consequently, the GDPR and DPA 2018 will need to be read side-by-side.

Data Protection Act

3. It is anticipated that the new UK DPA 2018 will be enacted into UK law by the 25th May 2018. The parliamentary Bill differs little from the GDPR except that it allows member states to enact domestic legislation in the following areas:

3.1 The management of information processing that falls outside EU law

3.2 The implementation of the Law Enforcement Directive which falls outside of the GDPR and deals with the processing of information for law enforcement

3.3 National security which falls outside of the remit if EU law

3.4 Domestic regulation, duties, powers and enforcement of the Act

3.5 The repeal of the predecessor Act and the interaction with the Freedom of Information Act/Environmental Information Regulations

4. The Bill is currently passing through the House of Lords before moving to the House of Commons for three further readings followed by Royal Assent.

5. The slow progress of this Bill has meant that UK bodies have so far not released some important guidance for organisations about how to implement the GDPR/DPA 2018 within the UK. Some helpful guidance is being released by the Article 29 working party, this group is made up of representatives of data protection authorities from each member state. The Trust has been advised that guidance will begin being published by the Information Governance Alliance and Information Commissioner's Office in early 2018. The effect of this has been that some Trust policies and procedures have not yet been updated and work on these will not be able to begin properly until 2018.

Organisational challenges

6. The IG department has undertaken a GAP analysis and mapped out the changes required by the organisation to ensure that it is ready for the impending change in legislation. This work has formed the basis of an action plan (see appendix one).

The paragraphs below set out the changes and how it is intended that these are met by the organisation.

Consent

7. 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. Where processing for patients and staff within the healthcare setting is concerned Article 6 of the GDPR provides express provisions for the processing of this data (see sections below). This means that the legal basis for collecting data in this instance will not be by the giving of consent by the data subject.

8. 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.

9. Article 6 (1) (e) 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.

10. There will still be occasions where it will be necessary for the organisation to seek informed, verifiable consent from individuals where the legal basis for processing of information will be consent. The IG will need to design a process where this can be captured.

Right to erasure

11. Article 17 of the GDPR provides data subjects with the new right to erasure providing one of the grounds set out in sections (1) (a – f) apply. In section 2, where a ground applies, the data controller needs to inform additional parties processing the data subject's data on behalf of the data controller about the right to erasure so that all evidence of data belonging to the data subject is erased.

12. However, the right to erasure is not automatic and section (3) (a – e) sets out further grounds which override the data subjects right to erasure. Specifically section 3 (b) which states that sections 1 and 2 will not apply for compliance with a legal obligation which requires processing by Union or Member State law or for the performance of a task carried out in the public interest. This will mean that patients will not have the automatic right to erasure of their medical records. Some rights to erasure will 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.

13. While the reduction of the scope of this right makes its implementation more manageable the challenge of identifying data sources that fall within the right to erasure persists. In response to this the IG department will endeavour to document all instances of processing via the Trust asset register as well as ensuring that once information is identified for deletion that a process is in place to ensure this happens in compliance with the law.

Information processing

14. Article 30 makes it mandatory for organisations to record 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.

15. 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 IG department is beginning to work with departments to ensure that the correct contract terms are in place.

16. Currently there are no standard NHS contract terms and the Trust will need to take legal advice to ensure that existing and new suppliers are bound by appropriate terms and that existing contracts are updated to adequately reflect the information processing which is being undertaken. The lack of standardised timely central guidance is being escalated via the SIGNS network to NHS Digital. It is anticipated that work to complete this exercise will be time consuming and if not completed by 25th May 2018 could pose a potential risk to the organisation. A risk based approach will be applied to completing this work which should hopefully provide some level of mitigation.

Subject access

17. Article 15 provides the right for individuals to obtain copies of information held about them by organisations. This is similar to the right already available within the DPA 1998. The main differences are that the timescale for complying with a request has changed from 40 calendar days to one month. A request for an extension of up to two months can now also be made. Under DPA 1998 the Trust could charge a fee for processing a request, no fee will be payable by the applicant under the GDPR. The only exception to this is where a request is manifestly unfounded, excessive or repeat copies of the same material are requested, in these cases a reasonable administration fee can be charged. The other main change is that organisations can refuse to process an application for information but must explain why to the individual, informing them of their right to complain to a supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

18. The main challenge envisaged from these changes is that the lack of chargeable fee may encourage an increase in applications. Currently the Trust is processing in excess of 500 applications for information per month. Each check involves verifying the identity of the requester, retrieving, checking and copying the material. In some cases involving searches of IT systems, the process can be protracted due to the need to seek consent from many data subjects cited in material such as emails.

19. Although the GDPR provides the ability to refuse requests in some circumstances no central guidance has been produced about how to administer the subject access process. It is anticipated that there will be guidelines which limit the circumstances in which a request can be refused and that this provision could have limited effect at reducing requests where the scope of the request is not refined.

Implementation progress so far

20. The Information Governance (IG) department has developed an action plan covering the main areas of work that are required to ensure that the Regulation/Act is implemented by the 25th May 2018 (see appendix one).
21. The IG department has been meeting with Divisions and areas such as human resources, procurement and Occupational Health who will be directly affected by the new legislation to explain the impact of the law and ensure that these departments are ready for May 2018.
22. Presentation materials have been produced and have been made available to staff on the IG intranet site.
23. The Trust information asset register has been updated to incorporate the data privacy impact assessment process, mandatory for all data processing under the new legislation. The department will begin actively promoting the logging of information assets in order to capture processing activity from early 2018, also mandatory under the new legislation.

Conclusion

24. A plan is in place to ensure that the Trust is ready for the implementation of the GDPR/DPA 2018 in May 2018. The process for preparedness has slowed due to the paucity of guidance from the Information Commissioner's Office and Information Governance Alliance. It is anticipated that guidance on areas such as privacy and subject access will be made available in early 2018 which will mean that this work can be finalised. It is anticipated that the Trust will be GDPR/DPA ready by the 25th May 2018. The only foreseeable risk will be ensuring that contracts with data processors are GDPR compliant.

Author: **Nuala Buchan Brodie**

Information Governance & Records Manager

29th December 2017

Appendix One – GDPR action plan

Action	Time-frame	Owner	Status
Consent			
Add field to EPR so that it can be verified that a patient has opted out of use of their data for secondary processing.	25/05/2018	Russell Dean Grant Vallance	
Check to see if added field could be overwritten with information from the Spine.	30/03/2018	Russell Dean	
Devise process for verification of consent.	30/03/2018	Simon Pillinger	
Right to be informed			
Re-write patient (adult/child) privacy notice following ICO best practice.	30/03/2018	Dr Chris Bunch	
Re-write staff privacy notice.	30/03/2018	Glyn Allington	
Include right to be forgotten process within privacy notice.	30/03/2018	Dr Chris Bunch/Glyn Allington	
Consult with children concerning draft privacy notice.	30/03/2018	Simon Pillinger	

Action	Time-frame	Owner	Status
Consult with staff group concerning privacy notice.	30/03/2018	Glyn Allington	
Right to be forgotten			
Identify major EPR systems and whether records can be deleted. **Need to identify other system outside patient records where right to erasure exists.**	30/11/2017	Nuala Buchan Brodie	Partially completed – not necessary because Trust's right to process data for health purposes overrides right to deletion.
Write process for individuals making a request for deletion of their information.	30/03/2018	Russell Dean	
The right to data portability and access to health records			
Re-write subject access request policy to include data portability.	30/03/2018	Nuala Buchan Brodie	
Explore whether access to patient portal provides adequate access to health records and would allow downloading of information to satisfy right to portability.	31/12/2017	Russell Dean	Completed – have asked that portal GDPR compliant with every page downloadable. Will only provide view only partial access to records.
Documentation of data processing			

Action	Time-frame	Owner	Status
Issue further communications concerning completion of information asset register.	Periodically through to April 2018	Simon Pillinger	
Contact departments directly to request population of information asset register.	Periodically through to April 2018	All	
Meet with procurement/commissioning to identify all examples of data processing.	28/02/2018	Nuala Buchan Brodie/Simon Pillinger/Russell Dean	Have met with procurement who are speaking with their network concerning change in legislation. Crown guidance produced in December 2017 setting out work.
Obtain copy of GDPR data processing agreement.	28/02/2018	Simon Pillinger/Mark Underwood	
Update contracts/re-issue and get signed data processing notices to organisations processing Trust data.	31/03/2018	Garry Walsh	
Data protection by design and by default			
Update data privacy impact assessment procedure.	31/03/2018	Simon Pillinger	Completed – to be presented to IGDQG in Feb 2018
Include data privacy impact assessment procedure as part of asset register.	31/12/2017	Simon Pillinger	Completed

Action	Time-frame	Owner	Status
Request retrospective completion of privacy impact assessments for information assets.	31/03/2018	All	Underway
Data protection officer			
Appoint data protection officer	25/05/2018	Peter Knight	Process started with HR and a suitably qualified individual is being identified.
Incident reporting			
Update incident reporting procedure to reflect new timescales.	25/05/2018	Nuala Buchan Brodie	Update completed – needs to be checked nearer 25/05/2018 to ensure still compliant.
Training			
Update induction and training to reflect new legislation.	25/05/2018	Russell Dean	
Information			
Fact sheets Consent for processing of non-clinically related data			
Develop information leaflet about changes to legislation and ensure this is available in	31/03/2018	Nuala Buchan Brodie	

Action	Time-frame	Owner	Status
all clinical areas.			
Create poster/leaflet for privacy notice. Add notes to internet/intranet sites re privacy notices Add new privacy notices for adults/children to site specific leaflets	25/05/2018	Simon Pillinger Russell Dean	
	25/05/2018	Simon Pillinger Russell Dean	
	25/05/2018	Simon Pillinger Russell Dean	
Write to all staff members via their pay slip concerning their information updated information rights.	25/05/2018	Glyn Allington	
Include staff privacy notice within induction materials.	25/05/2018	Glyn Allington	
Update information on Trust inter and intranet sites concerning data portability and subject access.	25/05/2018	Simon Pillinger/Russell Dean	
Promote the assessment of privacy impact via	Periodically from January 2018	Simon Pillinger	PIA are used currently in the Trust for new data flows. This is a good opportunity to reinforce

Action	Time-frame	Owner	Status
communications.			the use of the PIA.