The Royal Wolverhampton NHS
NHS Trust

Trust Board Report

Meeting Date:	Monday 26th February
Title:	Preparing for the General Data Protection Regulation 2016
Executive Summary:	The General Data Protection Regulation (GDPR) was passed in 2016 and fully comes into force on 25th May 2018. The Government has confirmed that the United Kingdom's decision to leave the EU will not affect the commencement of the GDPR in the UK. The UK Data Protection Bill is currently at the committee stage of Parliament, which will look to supplement the GDPR and clarify any derogations the UK has within some of the provisions of GDPR. This report provides the Trust Board with information about the GDPR and how the Trust is looking to implement this by May 2018.
Action Requested:	The Trust Board is invited to **receive** and **note** the new Data Protection requirements and the management actions being taken to prepare for the General Data Protection Regulation. The implementation of the Regulation is being managed through a dedicated group established through the Information Governance Steering Group.
For the attention of the Board	
Assure	• Provide assurance around the work that is being carried out in the Trust to support compliance with new regulatory requirements.
Advise	• Appendix 1 details progress against established work streams.
Alert	• The Data Protection Bill is yet to receive royal assent which may change or clarify some of the areas of the GDPR Regulation that allow for derogation. • The Supervisory body (Information Commissioner's Office) and other national bodies (Information Governance Alliance and NHS England) are slow to release sector specific guidance to support implementation.
Author + Contact Details:	Tel 01902 307999 Raz.Edwards@nhs.net
Links to Trust Strategic Objectives	1. Create a culture of compassion, safety and quality 2. Proactively seek opportunities to develop our services 3. To have an effective and well integrated local health and care system that operates efficiently
Resource Implications:	Loss of income from Subject Access fees. Workforce: New requirement for a Data Protection Officer function.

CQC Domains	**Caring:** staff involve and treat everyone with compassion, kindness, dignity and respect. **Well-led:** the leadership, management and governance of the organisation make sure it's providing high-quality care that's based around individual needs, that it encourages learning and innovation, and that it promotes an open and fair culture.
Equality and Diversity Impact	There are new provisions within the Regulation that require communication to be made in different formats and special consideration to communicating with children about how their data is used.
Risks: BAF/ TRR	n/a
Public or Private:	Public
Other formal bodies involved:	Information Governance Steering Group GDPR implementation group
NHS Constitution:	In determining this matter, the Board should have regard to the Core principles contained in the Constitution of: • Equality of treatment and access to services • High standards of excellence and professionalism • Service user preferences • Cross community working • Best Value • Accountability through local influence and scrutiny

Report Details

1 **Overview**

The GDPR comes into force across the EU on 25 May 2018 and will apply to the Trust as data controller, where we determine the purposes and means of processing personal data for both employees and patients, and also as data processors where we are responsible for processing personal data on behalf of another data controller.

The GDPR represents a step change in the way that data is protected and managed and the principles are consistent with, and extend the Data Protection Act 1998. GDPR introduces new rights for data subjects and strengthens existing rights available under previous laws.

This paper provides an overview of the Trust implementation plans to ensure compliance by the given deadline. Sector specific national guidance is being developed by NHS England but is not expected to be available until April 2018. Some guidance has already been issued by the Information Commissioner's Office (ICO) which provides an interpretation from a regulatory perspective. The Trust's activities in complying with these Regulations will focus on what can be delivered now, before 25 May 2018.

2 **Key requirements of GDPR**

a) **Fine enforcement** - 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 Euro, or 4% of annual turnover per breach.

b) **Accountability**- includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's elevates their significance.

- The Trusts governance measures need to be comprehensive but proportionate. Documentation of processing activities will become essential to support this requirement. Whilst we have started to adopt tools recommended by the ICO such as privacy impact assessments, privacy by design is now legally required in certain circumstances.

- Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although we already have good governance measures in place.

c) **Data Protection Officers (DPO's)** -. All public authorities must appoint a statutory Data Protection Officer. DPO's must be independent and must not be instructed on how to carry out this role within the organisation DPOs are not personally responsible in case of non-compliance with the GDPR. The DPO must report directly to the highest level of management (to a member of the Trust board). The Trust is currently looking at recruiting to this position.

d) **New Data Subject Rights**- On the whole, the rights individuals will remain under the GDPR is the same as those under the Data Protection Act 1998 but with some significant enhancements. Individual Rights are strengthened in relation to having inaccuracies corrected, having information erased, preventing direct marketing, preventing automated decision making and profiling and data portability, and having a wider right to be 'forgotten' than currently exists.

- **Privacy notices** - the right to be told is perhaps the right that is most

strongly enhanced, as this requirements 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 we 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 finalising the privacy notice and will be working with services to develop service specific notices to comply with this requirement.

- **Subject access requests (SAR),** under the current Data Protection Act, individuals can ask to see the information about them that is held by the Trust. This will change significantly under the GDPR:
  i. The timeframe for the provision of the requested information is being reduced from 40 calendar days to 30 days. The Trust is currently monitoring compliance in line with the 30 day timescale and anticipated that this will be achievable in readiness for May 2018.
  ii. There will be no more fees (£10 per request HR and £50 for Patient info) - with the removal of a fee there is an anticipated increase in request activity. Loss of revenue for charging fees for access to records. There are logistical implications of having to provide information within a short time frame and potential for increased work load given new right to data portability to provide information in an electronic format.

e) **Data Breaches** - all organisations are required to have procedures for reporting and investigating data protection breaches and legal obligation to inform ICO of serious breaches where the breach is likely to result in a high risk to the rights and freedoms of individuals. The Trust has existing procedures are in place including reporting to ICO, and will review the policy in readiness or May 2018 to ensure any new categories of breaches are reflected in the current reporting mechanism.

f) **Consent** - GDPR sets a very high standard for consent. 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. Where consent is obtained, the Trust must give affect the 'rights' associated with giving consent, which differ to those 'rights' afforded using data under a statutory provision. Therefore existing processing will need to be reviewed to identify either if there is a requirement for written consent or if there is another condition for processing to rely on.

g) **Privacy by Design** - data protection impact assessments or Privacy Impact Assessments (PIA's) will be routinely required for all new projects. The Trust is currently developing a tool that can be used to support this process.

h) **Information Asset Management** - The Trust is in the process of developing an asset register and mapping key information assets to ensure we fully document the personal data we hold, where it came from, who it is shared with and the legal basis under which it is used/ shared.

i) **Use of Data Processors** - The Regulation introduces liabilities for a data processor where they have failed to act on the instruction of the data controller. This will rely on ensuring appropriate contractual clauses are in place, explicitly stating obligations required for data processor, and ensuring these are monitored. Currently the Trust is reviewing contractual clauses and will be looking at issuing addendums where necessary. The Trust will also need to scope any processing where there are no contracts in place to ensure all processing is covered as appropriate.

Current Status

3	The Trust has established a GDPR working group to address the changes and ensure compliance, with leads for specific work streams across various disciplines. This work is overseen by the Chair who is also the Trust Caldicott Guardian. See Appendix 1 for detail of work streams. The gap analysis highlights that some significant changes are required; however it is anticipated that with the implementation of a robust action plan the Trust will be able to achieve compliance with the GDPR. A business case has been approved to supplement the Trust's existing Information Governance framework, programme and resources; to incorporate the required changes needed for the Trust to meet its obligations of the GDPR. Full implementation of the action plan rests on further guidance being published by the Information Commissioner for a number of areas. Activities will be staggered between those which can be taken now and those awaiting further guidance.
4	**Conclusion** The Trust has significant areas of work development ahead to ensure that systems and processes are put in place to meet the GDPR requirements as well as communicating what it means for staff and patients. Clarity on the interpretation of some of the requirements is needed before we can clearly identify what action we need to take as a Trust and the appointment of a DPO and adequately resourced IG function will be essential in supporting a smooth implementation as well as maintaining future compliance. Whilst there is a lot of work for the Trust, encouraging work is already underway in order to support compliance in readiness for May 2018, as detail in appendix 1.

Appendix 1

Key issue / GDPR Work stream	GDPR Implementation Group update	Next Actions	Timescales	Assurance level	Owner
1) Fair processing The right to be informed encompasses the obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how personal data is used.	Review of Trust wide privacy notice and communication methods to ensure compliance. Templates to be developed to assist specialists in publishing specific notices, once Trust notice has been agreed. Children specific notices are also now a legal requirement.	Ratification and publication of Trust wide privacy notice followed by a programme of work to establish service/ project specific notices.	March 2018		Health Records Manager
2) Rights of Access Individuals have the right to access their personal data and supplementary information with no free and within a shorter time scale (30 calendar days).The right of access allows individuals to be aware of and verify the lawfulness of the processing.	The Trust is currently assessing the impact the loss of income generated from subject access requests will have on performance within a shorter timescale. Anticipated increase in requests is also expected.	Review of OP07 to ensure new framework is reflected in current policy.	May 2018		Health Records Manager
3) Consent The GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance reputation. Consent requires a positive opt-in. No pre-ticked boxes or any other method of default consent.	The Trust needs to fully understand the GDPR consent guidance as it sets a much higher standard for consent. Currently lack of sector specific guidance in this area.	Development of a consent model to feature in review of OP07- Heath Records Policy	May 2018		Health Records Manager

4) Breach reporting The GDPR introduces a duty on organisations to report certain types of personal data breach to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.	The Trust currently has a robust incident reporting system. This is being reviewed to ensure timescales and categories of incidents are consistent with new GDPR requirements.	Review changes to breach reporting categories for GDPR and update OP10 – Risk Management Policy	April 2018		IG Manager
5) Data processor - contacts and compliance Whenever a controller uses a processor it needs to have a written contract in place. The contract is important so that both parties understand their responsibilities and liabilities. The GDPR sets out what needs to be included in the contract.	Map out all arrangements with commercial providers undertaking data processing; identify where formal contractual agreements are in place. Approach providers to request their plans to comply with the regulatory obligations to ensure compliance.	Drafting of new T&C's and issuing contract variations to identified suppliers.	March 2018		Head of Procurement
6) Privacy by design and Privacy Impact Assessments (PIA) Under the GDPR, the Trust is required to implement technical and organisational measures to show that we have considered and integrated data protection into processing activities. Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.	New protocol to be written to include privacy by design when building/ procuring new systems for storing or accessing personal data. A new tool is being tested to support conducting privacy impact assessments.	Testing and roll out of PIA tool – as well as embedding its use into system and practice across Trust.	April 2018		Head of Projects and Assurance, IT

7) Processing of children's data Children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved. When processing children's personal data it should be demonstrated how the organisations aims to protect them from the outset, and design your systems and processes with this in mind. Clear privacy notices for children are also required so that they are able to understand what will happen to their personal data, and what rights they have.	The Trust is currently assessing processing relating to children's data to review what impact this requirement is likely to have.	A children's specific privacy notice is under development.	May 2018		Directorate Manager Children's services
8) Data portability The right to data portability allows individuals/ data subjects to obtain and reuse their personal data for their own purposes across different services. This only applies were data is provided with consent or under the performance of a contract.	The Trust is currently assessing the need to fully comply with this requirement, due to lack of guidance issued in this area. In the meantime options are being explored to facilitate the ability to move, copy or transfer personal data from one IT environment to another.	System owners contacted regarding data portability. Evaluating the potential for an in-house solution for the provision of data from clinical web portal.	May 2018		Head of Projects and Assurance, IT
9) Profiling and automated decision making The GDPR has specific provisions on: a) automated individual decision-making (making a decision solely by automated means without any human involvement; and b) Profiling (automated processing of	The Trust currently assessing if and when this requirement would apply. Whilst such techniques may not be commonly utilised at present, it may become customary as technology and processing activities improve. At this stage the Trust is looking to establish a framework and model for this	Policy outline to be developed to satisfy the scope of this requirement.	May 2018		Information Manager

personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process	requirement.				
10) Mapping information assets and reviewing the basis for which we process.	The Trust has a comprehensive asset register which is being updated to be GDPR compliant. System owners are being established and risks/ legal basis for processing for each asset will be documented and reviewed. This will support compliance with the accountability principle of GDPR.	Detailed asset register in line with ICO guidance to be finalised and signed off.	May 2018		Head of Projects and Assurance, IT
11) Data subject rights, opt out, rectification, restriction. All rights available to data subjects should be communicated via fair processing notice and exercisable within 30 calendar days. • Right to be informed • Right to rectification • Right of access • Right to erasure • Right to restrict processing • Right to data portability • Right to object • Rights relating to profiling and automated decision making	To review current policies to ensure it meets with GDPR regulation and add to OP07 and communicate to all staff. To publish 'rights' as part of the privacy notice.	Incorporate 'rights' into policy review OP07 – Health Records Policy and ensure there is clear process for communicating rights to data subjects.	May 2018		Health Records Manager
12) Review data sharing agreements	A review of current data sharing agreements to ensure they are compliant and a review of the	Review of Wolverhampton overarching data	May 2018		IG Manager

	policy and templates to support future sharing.	sharing agreement, supporting policies and production of standard templates in line with GDPR.			
13) Policy review Full review of IG related policies to streamline and update in light of legislative changes.	To review policy structure of IG and data protection policies to consider how to improve and streamline/ relaunch.	Extraordinary policy group meeting arranged for end of Feb where plan will be presented.	Feb 2018		IG Manager
14) Communication/ Training and Awareness Raise awareness to staff and the public around the GDPR, what it means and how the organisation is complying with this.	IG manager has already carried out a number of briefings for key staff. Trust wide training will be available in readiness for deadline.	Delivery of targeted training and briefing sessions. Trust wide e-learning being developed.	April 2018		IG Manager
15) Accountability and governance and the role of the DPO The GDPR makes it a requirement that organisations appoint a data protection officer (DPO). The GDPR also contains provisions about the tasks a DPO should carry out and the duties of the employer in respect of the DPO.	Identification of options for a statutory data protection officer. To clarify the role/ function of the DPO. Communication of role an significance	Finalising job description.	May 2018		Medical Director / Caldicott Guardian
16) Pseudonymisation Processing personal data in such a way that data can no longer be attributed to a specific data subject without the use of additional information. This will allow organisations to utilise data whilst balancing the privacy of the data subject.	Whilst the Trust currently utilises such techniques, a formal process to be documented and governance of this is being considered.	New policy being drafted under umbrella IG policy to detail the use of this technique.	May 2018.		Information Manager

	GDPR sets out provisions in relation to this.					
	17) Processing implications in relation to employee data The GDPR requires the same considerations to be given to employee data that is afforded to patient data. This includes privacy by design, communication of fair processing and rights of access.	Work is needed to understand the types of employee data that is processed and how this should be communicated more effectively to staff moving forward. Formal processes to be established to address this requirement for staff processing.	Policies for staff to be reviewed to incorporate changes in regulation.	May 2018		Workforce manager