Item Number: 289.

GOVERNING BODY MEETING **Meeting Date: 4 August 2017**	NHS Scarborough and Ryedale Clinical Commissioning Group
Report's Sponsoring Governing Body Member: Philip Hewitson	**Report Author: Corporate Services Manager**

1. Title of Paper: New General Data Protection Regulations - Update

2. Strategic Objectives supported by this paper:
(check those which apply)

- ☐ To create a viable & sustainable organisation, whilst facilitating the development of a different, more innovative culture
- ☒ To commission high quality services which will improve the health & wellbeing of the people in Scarborough & Ryedale
- ☐ To build strong effective relationships with all stakeholders and deliver through effectively engaging with our partners
- ☐ To support people within the local community by enabling a system of choice & integrated care
- ☐ To deliver against all national & local priorities incl QIPP and work within our financial resources

3. **Executive Summary:**

The new General Data Protection Regulations (GDPR) will come into force from 25 May 2018. This paper informs the Governing Body of the action plan which is currently being worked through with support from eMBED. The Action Plan has been accepted by the Audit and Governance Committee

This paper supports the previous paper to the Governing Body in March which advised regarding the key changes in Data Protection legislation and identifies the risks associated with this for the CCG

4. **Risks relating to proposals in this paper:**

Whilst there is no concern at this stage that the CCG will not meet its requirements under the new regulations by May next year, there is a moderate risk that should we not meet the deadline the consequences would be a breach in our statutory duty with the risk of enforcement action and monetary penalties. Therefore the risk is included on the Finance and Contracting Risk Register

5. Summary of any finance / resource implications:

There is a financial risk associate with noncompliance with the regulations in the way of fines issued by the Information Commissioners Office (ICO).

6. Any statutory / regulatory / legal / NHS Constitution implications:

Compliance with the GDPR is a statutory duty enforced by the ICO

7. Equality Impact Assessment:

Not applicable

8. Any related work with stakeholders or communications plan:

Not applicable

9. Recommendations / Action Required

The Governing Body is asked to note the Action Plan

10. Assurance

As the risk has been identified as a 12 this will also be included on the Corporate Risk Register which will be monitored by Audit and Governance Committee and the Governing Body. The Audit and Governance Committee will monitor implementation through regular updates on the project plan which will be reflected in the risk register

For further information please contact:

Name: Emma Parker	*Title: Corporate Services Manager*	☎:01482 672191

MARCH 2017

GENERAL DATA PROTECTION REGULATION ACTION PLAN

Themes of the GDPR:

- Refining/tightening up of existing concepts
- Standardised law across the EU
- New concepts in regulation; accountability, demonstrating compliance, designing compliance
- Increased regulation/enforcement by ICO and data subjects
- Enhanced rights for data subjects
- Expectations of uniformity and portability

GDPR comes into force on the 25th May 2018 and the UK will still be a member state of the EU at that time.

The Information Commissioner's Office, the Information Governance Alliance and several other organisations are issuing guidance on an on-going basis.

This action plan will start to address the main issues and map out where changes need to be made.

Steps to take now	Items to be aware of	CCG Actions	eMBED Actions	Target Date
Raising Awareness	• Action plan to be presented to CCGs via IG Groups or other formal committees • SIRO to report to Board • Add update to regular IG reports • Comms to staff • Ensure accountability can be proven	Post IG Group Organisations to maintain records of processing activities – ongoing monitoring, reviewing and assessing processing activities to ensure compliance	eMBED to produce IG lead from eMBED to include update in regular reports eMBED to produce	July 2017 On-going September 2017
Information you hold	• No longer a requirement to register with the ICO – however each controller must keep records of its processing activities – these must be disclosed to the ICO on request • Comprehensive data flow mapping to include: What you hold Where it came from Who you share it with Legal basis for processing	SIRO to take responsibility for this SIRO to ensure that all areas map information and add in any new flows as they arise Confirm the legal basis being relied on	eMBED to assist with risk assessments where required eMBED to assist with identifying legal basis where required	On-going As required

	• Information Asset Register updated regularly	SIRO to ensure that all Information Asset Owners are updating the register and risk assessing existing and new assets on an on-going basis		On-going
Individuals' rights	Check procedures and policies and systems to ensure all the rights individuals have are covered including how to delete personal data or providing data electronically.		eMBED to recommend which procedures/policies require updating	September 2017
Subject Access Requests (SARs)	• Review and update Subject Access Procedures – no fees, time reduced to 1 month to respond • Ensure all staff dealing with SARs are aware of the new procedures • Need to explain legal basis for processing information and retention periods when responding to SARs (in addition to Privacy notices)	Inform all relevant staff	eMBED to update SARs procedure eMBED to produce template SARs response	March 2018 March 2018
Legal basis for processing personal data	Ensure all processing of data has a legal basis	SIRO to ensure this is included in data flow mapping		On-going
Consent	Consent must be explicit and requires clear affirmative action. It cannot be implied. A full record must be kept. Silence, pre-ticked boxes, inactivity or **failure to opt-out** do not constitute valid consent. Consent to the processing of personal data must always be clearly distinguished from other matters (e.g. cannot be wrapped up in other terms and conditions / consent to treatment etc.) Previously obtained consent will remain valid as long as it meets the GDPR standard	Identify all areas using consent as legal basis for processing and look at alternatives	eMBED to advise on consent forms and legal basis for processing	As required

	• Review of all areas where consent is used as the legal basis for processing and ensure adequate processes are in place	SIRO to ensure review takes place as data flow mapping and information asset register are updated		On-going
Children	• Ensure that processes are in place for recording consent of parent or guardian where appropriate (children under 13) • Add in section to Privacy Notice in a clear, plain way that a child can understand about their consent or produce separate notice for children	Organisation to ensure processes are in place Organisation need to identify whether necessary		March 2018 March 2018
Data breaches	Ensure that all staff are aware that breaches must be reported within 72 hours and that there is a new duty to inform data subjects of high risk breaches. Comms to staff. Ensure incident reporting policy and procedures are clear and well-practised to ensure quick response to any breaches Data subjects have the right to compensation from a data controller or data processor	Ensure processes are in place and all staff are made aware.		March 2018
Data Protection by Design and Data Protection Impact Assessments	Embed the Privacy Impact Assessment process within the organisation Any new systems or processes should be commissioned and built using data protection by design and by default.	SIRO and project leads IT, project teams and commissioning teams need to be aware	eMBED to provide advice on completion of PIAs and risk assessments of PIAs where necessary	ASAP September 2017

	Requirement to consult with the ICO in advance where a data impact assessment indicates that the processing would result in a high risk if measures are not taken to mitigate that risk CCTV or health monitoring systems must have a PIA	 Organisation to check	eMBED to advise on any high risk processing	 September 2017
Data Protection Officers	All public bodies must have a data protection officer who takes responsibility for data protection compliance • Must have expert knowledge • Must report directly to the board Must be independent (can be a contractor) – a group of public authorities may collectively appoint a single DPO (as long as the DPO is accessible to all)	Organisation to make a decision on how to proceed with this	eMBED to advise on the requirements of the role	May 2018
New duties for data processors	• Data processors become data controllers if they act beyond instructions • Restrictions on sub-contracting by data processors • Must have clear contractual provisions • Data processors can now be fined	Check all existing data processor contracts for compliance. Organisations to ensure all data processors have contracts in place and are IGT level 2 compliant		September 2017 September 2017
Fair Processing Notices	Must be transparent and easily accessible. Concise form. Must include: • Contact details of the data controller • Contact details of the Data Protection Officer • Legal Basis	Review whether separate privacy notice is required for children	eMBED to work with organisation to review privacy notices	September 2017

	• Data retention period • Reference to the rights of erasure, rights to withdraw consent, to object to processing, data portability and to complain to the ICO Revisit fair processing notices for staff – don't rely on consent	Where records are held areas to check data retention periods as these will need to be added in. Review data sharing agreements to ensure data subjects are being provided with all the relevant information. HR to review contracts		
Audits	Additional powers granted to the ICO will allow them to: • Carry out audits • Issue orders to cease operations • Notify data subjects of a breach • Restrict or erase data • Suspend or prohibit processing or order suspension of data flows to third countries Need to ensure all the above actions are completed before May 2018	Organisations need to ensure that they can **demonstrate** compliance in all areas of the GDPR – with **evidence** that it is meeting its obligations		On-going