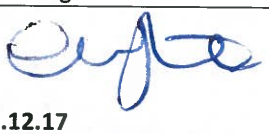
NHS
North Lincolnshire
Clinical Commissioning Group

Date:	14th December 2017
Meeting:	Governing Body
Item Number:	8.4
Public/Private:	Public ☒ Private ☐

Author: *(Name, Title)*	John Pougher Head of Governance
GB Lead: *(Name, Title)*	Catherine Wylie Director of Quality & Nursing
Director approval/signature (MUST BE SIGNED) Date:	 **5.12.17**

Report Title:
General Data Protection Regulation (GDPR) – Briefing paper
Decisions to be made:
To Note

Continue to improve the quality of services	☐	**Improve patient experience**	☐
Reduced unwarranted variations in services	☐	**Reduce the inequalities gap in North Lincolnshire**	☐
Deliver the best outcomes for every patient	☐	**Statutory/Regulatory**	☒

Executive Summary (Question, Options, Recommendations):

The CCG must be compliant with GDPR by 25 of May 2018. The CCG's Information Sub -Group monitors the GDPR compliance plan, with specialist support provided by EMBED. An Assurance report will go to the January meeting of the CCG's Quality Group. Whilst the CCG is currently 'on track' to meet requirements; a Data Protection Officer still needs to be appointed. This key post is likely to be delivered through some form of shared arrangement and will have a financial cost for the CCG. The attached paper outlines the key requirements of the new legislation.

Equality Impact	Yes ☐ No ☒	
Sustainability	Yes ☐ No ☒	
Risk	Yes ☐ No ☒	
Legal	Yes ☒ No ☐	Compliance with GDPR is a legal requirement. A breach of the regulations could result in a significant fine for the CCG and /or individuals.
Finance	Yes ☐ No ☐	

Patient, Public, Clinical and Stakeholder Engagement to date									
	N/A	***Y***	***N***	***Date***		***N/A***	***Y***	***N***	***Date***
Patient:	☐	☐	☐		**Clinical:**	☐	☐	☐	
Public:	☐	☐	☐		**Other:**	☐	☐	☐	

GENERAL DATA PROTECTION REGULATION (GDPR) - Briefing Paper

Background

The Governing Body is responsible for ensuring that the CCG will be compliant with GDPR legislation and should therefore be aware of the main new requirements and the CCG's current position. Note: GDPR comes into force on the 25th May 2018.

Key GDPR Principles

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act. The regulation however strengthens the principles of data protection by putting more focus on accountability and security. Organisations processing personal data will be obliged not only to comply with the new law, but also to demonstrate that they have complied. This principle of accountability is an important and significant shift change from passive to active compliance.

CCG Current Position

The CCG's Information Sub-Group (which reports into the CCG Quality Group) has been responsible for agreeing and monitoring progress against the IG work plan - which incorporates the GDPR compliance plan. Specialist support is provided to NL CCG by EMBED who also support a number of local CCG's. The CCG is currently on track to declare compliance for May 2018. In January 2018 an assurance report, detailing actions completed and overall progress will be reviewed by CCG's Quality Group.

In common with all public bodies the CCG must appoint a Data Protection Officer (DPO) to lead on the implementation of the new law. This is a specialist post and the organisation must ensure that the Officer appointed has proven expert knowledge of data protection law and practices.

Most CCG's are seeking to make a shared appointment. EMBED are currently preparing a proposal for a shared post across local CCG's. Other potential offers should be available in the near future. The Governing Body should note that there will be a financial cost associated with the appointment of a DPO however this should not be significant for a shared post.

GDPR Main requirements:

1. **Information held**

- There will no longer be a requirement to register with the ICO
- Comprehensive records must be kept of all data processing activities – the CCG must be able to show accountability and prove compliance
- The CCG must implement appropriate security measures such as policies, staff training, compliance checks
- The CCG must implement measures that meet the principles of data protection by design and default e.g. Privacy impact assessments for new processes or systems and these should be conducted at an early stage
- The CCG must adhere to approved codes of conduct
- Data flow mapping and the CCG Information Asset Register must be kept up to date

2. Individual's Rights

- Fair processing/Privacy notices must be kept up-to-date to ensure fair and lawful processing
- Right of data portability
- Right of erasure
- Right of rectification
- Right to object to and restrict processing
- The CCG needs to check procedures, policies and systems to ensure that all the rights can be covered

3. Subject Access Requests

- No longer able to charge any fees (some circumstances where you could charge an administration fee)
- Shorter time scale – only 1 month to provide information
- Need to explain legal basis for processing information and retention periods when responding to SARs
- New duty to help data subjects exercise their rights
- Requests can be refused if they are *'manifestly unfounded or excessive'*
- Responses also need to include details of other data protection rights and the ability to complain to the ICO
- The CCG will need to review Subject Access Procedure and inform relevant staff

4. Legal Basis for processing personal data

- To process any personal data an organisation must have a schedule 2 condition (now article 6).
- To process sensitive personal data (now special category data) the organisation must also have a schedule 3 condition (now article 9)
- Medical purposes condition has been expanded to expressly include both health and social care. This applies to treatment and management of services.
- Data flows must show which legal basis the CCG is relying on to carry out the processing
- Consent is not always the best condition to rely on, others such as' necessary for the performance of a contract' may be more suitable
- Review legal basis for all processing

5. Consent

- Review how the organisation seeks, obtains and records consent
- Must be freely given, specific, informed and unambiguous
- Must be a positive indication of agreement – cannot be inferred from silence, pre-ticked boxes or inactivity
- Must be able to demonstrate that consent was give – effective audit trail
- Individuals have a right to withdraw consent at any time

6. **Children**

- Need to be able to verify individuals' ages and gather parental or guardian consent if under 13
- Consent must be verifiable
- Must have a privacy notice written in language that children will understand
- Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child
- Review how consent is obtained and recorded

7. **Data Breaches**

- Duty on all organisations to report certain types of data breach to the relevant authority and in some cases to the individuals affected where the breach is likely to result in a risk to the rights and freedoms of individuals
- Must notify within 72 hours
- Failure to notify can result in an additional fine of up to €10m or 2% of global turnover
- Fines for a breach will increase to up to €20m or 4% of global turnover
- Individuals can also be fined
- Vital to ensure that staff understand what constitutes a breach and that a reporting procedure is in place and widely recognised
- Review incident reporting policy and inform all staff of changes

8. **Data Protection by Design**

- Obligation to implement technical and organisational measures to show that the CCG has considered and integrated data protection into processing activities
- Should be linked to other process such as risk management, IT and project management

9. **Data Protection Officers**

- All public bodies and organisations whose activities involve the regular and systematic monitoring of data subjects on a large scale must have a Data Protection Officer (DPO) who takes responsibility for data protection compliance
- DPOs inform and advise the organisation, monitor compliance and carry out audits, advise on PIAs, be first point of contact for supervisory authorities and data subjects
- Should report to the board, operate independently, not to be dismissed for performing their task and should have adequate resources to meet GDPR obligations
- Need to have professional experience and knowledge of data protection law

10. **New duties for data processors**

- GDPR places new specific legal obligations on data processors
- Required to maintain records of personal data and processing activities
- Significantly more legal liability if you are responsible for a breach
- Data processors can now be fined
- Must ensure contracts are in place between data processors and data controllers
- Data subjects have a right to receive compensation from data controllers and data processors if damage is suffered
- Review all data processor activity and check contracts are in place

11. Fair Processing/Privacy Notices

- Must be transparent and easily accessible and in a concise form
- Must include contact details of DPO
- Must include legal basis for processing
- Must include data retention periods
- Must reference the data subjects rights
- Review notices for staff
- Review existing notices
- Review whether separate fair processing notice required for children

12. New ICO Powers

- Additional fines
- Carry out audits
- Notify data subjects of a breach
- Restrict or erase data

December 2017