Working with you to make Sheffield HEALTHIER

NHS Sheffield Clinical Commissioning Group

General Data Protection Regulation (GDPR)

Governing Body meeting

H

24 May 2018

Author(s)	Sandie Buchan; Head of Information, Performance and PMO
Sponsor Director	Brian Hughes; Director of Commissioning and Performance

Purpose of Paper

On 25 May 2018, new data protection legislation comes into force under the remit of the General Data Protection Regulation (GDPR). The Information Governance team have been preparing the organisation to be compliant with all of the new regulations. This paper outlines the key components of GDPR and provides assurance on the preparedness of Sheffield CCG.

Key Issues

All organisations that handle and hold personal sensitive information have to legally abide by new data protection legislation from 25 May 2018. NHS organisations already comply with a number of data protection areas that GDPR has now imposed on all organisations, however there are a few key changes that Sheffield CCG has been required to implement across the organisation.

Actions have been taken to ensure all staff are aware of the changes in practice and what they now need to do to be compliant. This includes:

- What type of information is held
- Individual's rights
- Consent
- Data breaches
- Data protection by design
- Data processors
- Data Protection Officer

Work continues to ensure all necessary changes are embedded and regular reviews of data will become business as usual under the remit of GDPR.

Is your report for Approval / Consideration / Noting

Consideration and Noting

Recommendations Required by Governing Body

The Governing Body is asked to note the information as detailed within this paper on the key components of what GDPR means to Sheffield CCG and the actions that have been undertaken to date. As part of the internal audit process, an audit has been completed on the CCG's preparedness for the implementation of GDPR in which the level of assurance is yet to be returned. A further audit will be completed in the summer, on the CCG's

compliance of the legislation.

The Governing Body is asked to take assurance on the steps that the Information Governance team have taken to ensure compliance to the new GDPR legislation and ongoing review of all data and information within the organisation.

Governing Body Assurance Framework

Principal Risk: 5.4 Inadequate adherence to principles of good governance and legal framework leading to breach of regulations and consequent reputational or financial damage.

Are there any Resource Implications (including Financial, Staffing etc)?

No

Have you carried out an Equality Impact Assessment and is it attached?

Please attach if completed. Please explain if not, why not
Not required as this is an update paper

Have you involved patients, carers and the public in the preparation of the report?

Not required as this is an update paper

NHS
Sheffield
Clinical Commissioning Group

General Data Protection Regulation (GDPR)

Governing Body meeting

24 May 2018

1. Introduction

1.1. On 25 May 2018, new data protection legislation comes into force under the remit of the General Data Protection Regulation (GDPR). The NHS already complies with a number of data protection areas that GDPR has now imposed on all organisations that handle and hold personal sensitive information, however, there are a few key changes that Sheffield CCG has been required to implement across the organisation. Fines for non-compliance can be up to €20,000,000 or 4% of international turnover of the organisation.

1.2. This paper details what the key components of GDPR are, what this means for Sheffield CCG and what actions have been taken to ensure compliance.

2. General Data Protection Regulation key components

2.1. Information we hold

Under this new legislation, comprehensive records must be kept of all data processing activities whilst showing accountability and proving compliance. This means that all data flows and information assets are reported, detailed and kept up to date. All organisations must be able to demonstrate that appropriate security measures are in place such as policies, staff training and compliance checks in the form of regular reviews and updates.

As part of Sheffield's CCG annual Information Governance Toolkit submission, all data flows and information assets are reviewed and reported whilst ensuring that identified leads have relevant training. The Information Governance team will now be taking a more proactive stance throughout the year to ensure that data flows and the information asset register remain up to date at all times. Therefore, assurance can be given to Governing Body that the organisation is compliant in this area.

In the last few months whilst GDPR guidance has been released, the Information Governance team have been reviewing and updating relevant policies which a number have been approved by the Governance Sub-Committee. There is a schedule of policy reviews which identifies which policies will be updated in the up and coming months to ensure compliance in all areas in regards to GDPR.

As of 14 May 2018, 94.5% of all Sheffield CCG staff have been trained in the new Data Security and Protection mandatory training.

2.2. Individual's Rights

One of the main purposes of the new GDPR legislation is to extend individual's rights on information that is held about them. The NHS has always granted patients access to the information that is held about them in the form of Subject Access Requests (SARs). Following the implementation of GDPR, an individual's rights are extended to include:

- Rights of access to data
- To have inaccuracies corrected
- To have information erased where inaccurate
- To prevent direct marketing
- To prevent automated decision-making and profiling
- Data portability

The Information Governance team have been communicating to all staff in the form of Directorate presentations, drop-in sessions and regular weekly communications, what this means to them and their particular work areas. Further training is being planned for teams such as Continuing Healthcare and Complaints where these requests will be more prominent.

2.3. Consent

Under GDPR, consent must be freely given, specific, informed and unambiguous, therefore the Information Governance team have been preparing template documents on how teams and commissioning portfolios can gain consent under these new rules for future transformational programmes and service reviews. All areas have been informed that consent cannot be inferred from silence, pre-ticked boxes or inactivity and that all actions involved in obtaining consent requires recording.

A particular issue around gaining consent from carers has been raised within the organisation and processes have been developed to ensure that all members of staff adhere to the required regulations.

2.4. Data Breaches

Sheffield CCG already has an incident reporting policy, however under GDPR, the main change is that all major data breaches must be notified to the Information Commissioners Office (ICO) within 72 hours of the breach. This is a very tight turnaround and whereas the organisation is not operational during the weekend, processes have required to be tightened up. Failure to notify the ICO within this timeframe can result in an additional fine of up to €10m or 2% of global turnover.

This requirement has been presented to all Directorates and additional training is being offered on how to report incidents and what to do when a breach is identified. The Information Governance team will be leading this training and being the point of call for all incident related queries for Sheffield CCG.

2.5. Data Protection by Design

Data Protection is now to be considered through all processes and systems where personal data may be sought. Therefore, Sheffield CCG has approved a Data

Protection Impact Assessment (DPIA) that is being used throughout South Yorkshire and Bassetlaw, which its inception has been led by eMBED. This newly adopted DPIA will become part of the Programme Management Framework within Sheffield CCG and be completed alongside any programme or project business case.

2.6. Data Processors

GDPR places new specific legal obligations on data processors. Therefore Sheffield CCG now must have contracts in place with all data processors and any organisation that is commissioned to carry out work on behalf of the CCG. This should include a very clear "data processing agreement" to manage risks with suppliers/subcontractors.

Sheffield CCG has been reviewing all main contracts and data sharing agreements to ensure that they meet all GDPR requirements moving forwards.

Smaller non-NHS contracts are currently being reviewed to ensure that they are GDPR compliant, however as some of these relate to individual patient's care delivery, this is a significant task and will remain ongoing past 25th May 2018.

2.7. Data Protection Officer

Another requirement under GDPR is the need for Sheffield CCG to have a Data Protection Officer (DPO). The purpose of a DPO is:

- The DPO has knowledge of data protection law and practice and will advise the data controller and processor of their legal obligations, as well as provide guidance on how to monitor compliance on all aspects of GDPR and other data protection laws and regulations
- The DPO role is designed to be independent
- The DPO is the key accountable individual for GDPR and as such will respond to requests and be the point of contact for the Information Commissioner's Office (ICO)
- This is a public facing role and the public can raise issues with the DPO
- There is a requirement for the DPO to have an independent reporting line and be empowered to report directly to the Board without interference.

The CCG have formally agreed to appoint a DPO through eMBED for a period of two years. There is a formal contract in place in which the requirements of the DPO and the level of involvement with the CCG will be monitored and reviewed on a regular basis. Due to this role being extremely new, the level of need is not yet known, therefore after discussions with other CCG's within South Yorkshire and Bassetlaw, it was decided to be offered to eMBED for a trial period of two years.

3. Recommendations

The Governing Body is asked to note the information as detailed within this paper on the key components of what GDPR means to Sheffield CCG and the actions that have been undertaken to date. As part of the internal audit process, an audit has been completed on the CCG's preparedness for the implementation of GDPR

in which the level of assurance is yet to be returned. A further audit will be completed in the summer on the CCG's compliance of the legislation.

The Governing Body is asked to take assurance on the steps that the Information Governance team have taken to ensure compliance to the new GDPR legislation and ongoing review of all data and information within the organisation.

Paper prepared by Sandie Buchan; Head of Information, Performance and PMO

On behalf of Hughes; Director of Commissioning and Performance

14 May 2018