Bristol, North Somerset and South Gloucestershire
Clinical Commissioning Group

BNSSG CCG Governing Body Meeting

Date: Tuesday 1st May 2018
Time: 1.30pm
Location: The Winter Gardens Pavilions, Weston College, 2 Royal Parade, Weston Super Mare BS23 1AJ

Agenda item:

Report title: Report on the preparedness of the BNSSG CCG for General Data Protection Regulations (GDPR)

Report Author: Maxwell Allen
Report Sponsor: Sarah Truelove and Mike Vaughton

1. Purpose

This paper describes the preparations for the new legislation.

2. Recommendations

Note the report

3. Background

The General Data Protection Regulation (GDPR) comes into effect on May 25th 2018. Along with the new Data Protection Bill currently being debated by the UK Parliament, this legislation will replace the Data Protection Act 1998.

It will be a legal requirement for the BNSSG CCG to adhere to the new legislation.

This is the biggest change to data protection legislation in over 20 years. This change will alter many aspects of how the CCG manages, reports, and documents its use of confidential data. The overarching principles of Data Protection will not change, however the GDPR and the new Data Protection Act aim to keep people's data safer and to give people more rights over how their personal information is used.

Organisations that breach the new Data Protection legislation could receive higher fines than in the past.

While the challenges may seem unnerving, it's important to remember that all NHS organisations have, for many years, abided by their regulatory requirement to submit an IG

Toolkit each year. So while there will be important changes, there will also be many elements that we are all familiar with and that are already imbedded into NHS culture.

But no matter how well prepared we may think we are, the fact remains there will be changes and it's important that the NHS, in all its forms, strives to meet the challenges of good data management in a rapidly changing technological and landscape.

4. How is the CCG preparing for GDPR?

4.1 Policies

A new suite of Information Governance policies are being prepared by the CSU to comply with GDPR and the new Data Protection Act. These will soon be available for the CCG to formally adopt.

However, these policies cannot be finalised by CSU until the Data Protection Bill receive Royal Assent.

A delay has been caused by the UK Parliament which has not yet approved the Data Protection Bill. At the time of writing this report the Data Protection Bill has been considered at the Public Bill Committee and is due to be considered at the "Report" stage (meaning the Whole House, either the House of Commons or the House of Lords, must review the amended form of the Bill and then make further changes). It is then required to have its Third Reading (meaning that a Bill must be passed in each House before it can become law. It is normally the final opportunity for the Commons or the Lords to decide whether to pass or reject a Bill in its entirety).

Senior CSU staff are monitoring the situation and the CSU and CCG organisations are working closely together to ensure there is no delay. As soon as there is certainty on the government position the policies will be delivered. However, it's very clear that there is little benefit in approving the policies at this stage when they may require alteration in a number of weeks.

4.2 Data Protection Officer

The GDPR legislation requires that an appropriate staff member at the CCG is nominated to the role of Data Protection Officer.

The role of Data Protection Officer is mandated by GDPR to monitor compliance to the legislation, advice on data protection, and act as a central point for data subjects.

While the role has yet to be officially nominated by the CCG, the CSU have advised they will support the nominated employee within current SLA arrangements.

4.3 Information Asset Register and Data Flow Map

Monitoring and documenting data flows and information assets will be a cornerstone of compliance to the GDPR

Historically, maintaining an Information Asset Register and Data Flow Map have always been a key part of mandated IG requirements for CCGs.

The Information Asset Register contains a list of all the information systems that hold confidential data. The Data Flow Map must contain a list of data that is flowing in and out of the organisation.

The information asset register and data flow mapping activities assist with demonstrating compliance with GDPR. . For example, if required to do so by the ICO, organisations must be able to evidence the legal basis and purpose to process confidential data they are responsible for.

While the CCG has made a great deal of progress in this area over the last year, there is still more work to do to ensure these documents remain relevant and comprehensively detailed, especially in terms of risk assessing the use of data on an ongoing basis.

4.4 Information Asset Owners

Information Asset Owners (who are staff that look after systems that contain confidential data) will continue to play a key role in ensuring the CCG is GDPR compliant.

Contained within the Information Asset Register is the name of each asset owner. It is the responsibility of each asset owner to report any risks associated with their information asset and to report on the exact nature of the processing taking place.

However, suitable engagement and a clear reporting structure are required to facilitate this. Information Asset Owners must receive the appropriate support and guidance to be able to report accurately.

Without the support of the Information Asset Owners it will not be possible to maintain a clear picture of the processing taking place, and therefore gaining the evidence required to prove compliance to the GDPR will be more difficult.

The CSU will engage with Information Asset Owners to offer specialist support and provide tailored awareness sessions, while the organisational structure of the CCG will need to facilitate clear mechanisms for the asset owners to report on their processing status. For example, by ensuring they are kept informed of relevant group minutes and papers.

4.5 Organisation structure

The organisational structure of the newly formed CCG will include the creation of an IG group that will meet regularly to oversee compliance to the GDPR.

A new Terms of Reference is currently being drafted by the CCG to detail the remit of a new IG group that will meet monthly or bi-monthly to ensure the organisation is compliant to GDPR. Key staff, such as the Caldicott Guardian, SIRO, IG Manager, Data Protection Officer, and departmental leads will be required to make up the corum.

While the exact structure of the meetings has yet to be finalised, senior staff have met regularly to ensure any gaps in compliance are identified early during the transition period.

4.6 IG Toolkit submission (version 14.1)

The IG Toolkits have been submitted for the three CCGs that have now made up the newly merged single CCG.

The IG Toolkits provide assurance that organisations are well positioned to protect confidential data. The IG Toolkits scored satisfactory across the three CCGs. The IG Toolkits will remain separate for each CCG until the next submission date, as the last submission date occurred prior to formal validation of the newly formed CCG.

A new single toolkit for the newly formed CCG will be submitted in March 2019.

The current scores for the three previously separate CCGs are:

Bristol – 82%
North Somerset – 82%
South Glos – 81%

4.7 IG Training for staff

At least 95% of all the CCG staff must be compliant with their IG training.

All CCG staff will need to be aware of GDPR and their obligations and responsibilities for data protection. The CCG intends to develop and foster a culture that actively promotes and supports staff to fulfil the requirements for data protection.

It's a regulatory requirement that that at least 95% of staff have done their IG training, which include many components they will need to ensure they treat confidential information appropriately.

Currently the organisation is complaint with this requirement.

Further work will be required to maintain this status by ensuring staff retake their training in plenty of time before submission of the next IG toolkit.

5. Financial resource implications

None

6. Legal implications

General Data Protection Regulation (GDPR)
Data Protection Bill

7. Risk implications

A breach of data protection could lead to fines, reputational damage, and loss of trust in the organisation.

8. Implications for health inequalities

None

9. Implications for equalities (Black and Other Minority Ethnic/Disability/Age Issues)

None

10. Consultation and Communication including Public Involvement

None

11. Appendices

None

Glossary of terms and abbreviations

Please explain all initials, technical terms and abbreviations. For guidance please refer to the Jargon Buster and the CCG's Master Glossary – both are available on the website.

GDPR	In order to ensure the laws that oversee all our personal data are adequate, the EU have created the General Data Protection Regulation (GDPR). It will change how businesses and the public sector handle personal information. The Information Commissioner's Office provides a range of supporting documents on GDPR: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
IG Toolkit	The Information Governance Toolkit is a Department of Health (DH) Policy delivery vehicle that NHS Digital (formally the Health and Social Care Information Centre) is commissioned to develop and maintain. It draws together the legal rules and central guidance set out by DoH policy and presents them in in a single standard as a set of information governance requirements. The organisations in scope of this are required to carry out self- self-assessments of their compliance against the IG requirements and submit the results via the IG Toolkit website.. https://www.igt.hscic.gov.uk/