GDPR Briefing Paper

Background

The General Data Protection Regulation (GDPR) is the regulation by which the European Parliament, the Council of the European Union and the European Commission are strengthening and unifying data protection for all individuals within the European Union (EU).

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The GDPR applies to both Data Controllers and Data Processors. The definitions are broadly the same as under the DPA – i.e. the data controller says how and why personal data is processed and the processor acts on the data controller's behalf.

Unlike the current Data Protection Act (DPA), the GDPR places new specific legal obligations on data processors, allocating significantly more legal liability if they are responsible for a breach. However, this does not absolve data controllers of their obligations where a data processor is involved. The GDPR places further obligations on data controllers to ensure that contracts with data processors comply with the GDPR.

The GDPR applies to the processing of personal data carried out by organisations operating within the EU and also to processing carried out by organisations outside the EU that offer goods or services to individuals in the EU.

What changes under GDPR?

The GDPR is only relevant where processing personal data. Pseudonymised data processed by the CHCs is unlikely to fall within GDPR.

Also, it should be recognised that the responsibility and accountability for implementing the GDPR lies at an organisational level with those that are controllers or processors of personal data. For CHCs it is important that you liaise with your host organisation to ensure that you work together to implement that changes required. The following guidance is intended to assist with that process.

Finally, organisations processing NHS personal data are already required to comply with the requirements set out under the relevant IG Toolkit for their organisation. This should place them in a reasonable position with regards to compliance with the GDPR.

Domestic legislation will be required for locally-allowed derogations, where each member state has leeway to interpret how issues will be implemented, of which there are around 50.

Appendix 1 provides links to further information and guidance that is currently available and they will be updated over time. The key issues and actions required are summarised here.

Personal Data

The definition of personal data in the GDPR has been expanded to reflect changes in technology and the way organisations collect information about people. Information such as an online identifier – e.g. an IP address – can be personal data. As with the DPA, the GDPR applies to personal data held electronically or in manual filing systems. Information that falls within the scope of personal information under the DPA will also fall under the GDPR definition.

Of key importance to the CHCs is that personal data that has been pseudonymised can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual. Discussions about exactly what this will mean in the UK are ongoing and advice is expected soon.

Sensitive personal data

The GDPR refers to sensitive personal data (which includes health data) as "special categories of personal data". These categories are broadly the same as those in the DPA, but there are some minor changes. For example, the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Accountability

Controller organisations are required to have effective policies and procedures for handling personal data under the GDPR, to monitor compliance, and to assess their effectiveness. There should also be an effective management structure with needs based training provided to staff. Appropriate technical and organisational measures to protect data will be required.

This is a requirement of the IG Toolkit although existing policies and procedures will need to be reviewed in light of the new requirements of the GDPR. These records must be made available to the ICO on request.

Information the Organisation Holds

Controller organisations will need to document the personal data they hold, where it came from, who it is shared with, retention periods and the legal basis for processing.

A robust information asset management (IAM) process is a requirement of the IG Toolkit although current asset registers and data flow mapping may not incorporate the legal basis for processing. As for Accountability, these records must be made available to the ICO on request.

Additionally, there is an obligation on organisations that have shared inaccurate data with another organisation to tell them so they can correct it.

Data Protection by Design.

Organisations must ensure that current technical and organisational measures are appropriate to protect data that they process.

Privacy Impact Assessments under the DPA are renamed Data Protection Impact Assessments (DPIA). Under GDPR they become a legal requirement when high-risk data processing is involved. High risk processing will include automated processing and profiling which affect the subject and large-scale processing results of special categories of data (which includes health data). Organisations must assess when a DPIA is required and this must be linked to existing organisational risk management and project management processes.

Where a DPIA indicates high-risk data processing there will be a requirement to consult the ICO to seek its opinion as to whether the processing complies with the GDPR.

The use of PIAs is a requirement of the IG Toolkit although many organisations may not routinely undertake them. It is likely that DPIAs will be required to be undertaken retrospectively for existing processing activities as well as any future project plans.

Data Protection Officer

All public authorities and public bodies must designate a Data Protection Officer to facilitate compliance with the GDPR and ensure that they are appropriately trained. DPOs are not personally responsible in case of non-compliance with the GDPR. Data protection compliance is a responsibility of the controller or the processor. The DPO role is protected, they must report to the highest authority and cannot be dismissed or penalised for performing their rolw.

The DPO role includes:

- Compliance monitoring for policies and procedures
- Identification of the requirements for; and assessment of the results of a DPIA
- Act as a contact point for the ICO
- Advise the controller on a risk-based approach to processing
- Keep appropriate records of processing activities

For many organisations, it is likely that the IG manager will take on the DPO role.

Privacy notices and Transparency

As currently mandatory for the DPA, the organisation will be required to effectively communicate to subjects about the processing they undertake. This must now be given to data subjects and must include the legal basis for processing their data, as well as the retention periods used and that they have the option to complain to the ICO if required. The notifications must be easy to understand, particularly for children.

Privacy Notices are widespread throughout the NHS, however, the ICO has updated guidance on the subject (see Appendix 1) and existing notices will need to be reviewed in light of the new guidance. Further sector specific guidance can be expected from the IGA.

Consent

Note: The NHS do not usually require consent to process data under the DPA they rely on legal basis to do so. Consent as we refer to it is usually to address common-law duty requirements not data protection requirements. The legal basis to process data under GDPR is similar to that under the DPA.

The ICO, as the Data Protection Regulator, has advised organisations to review how they seek, obtain and record consent. Gaining consent to comply with GDPR will be harder, and subjects have stronger rights to have their data deleted if consent is used as the legal basis for processing. Consent will have to be freely given, specific, informed and unambiguous, not inferred from silence, pre-ticked boxes or inactivity.

Data Controllers must be able to demonstrate that consent was given via an effective audit trail. In addition, where consent is used to process data about children, procedures to verify the ages of children under 13 and to gather parental / guardian consent for processing their data will be required. This, too, will need to be verifiable.

Sector specific Guidance is expected from the IGA. Organisations will need to be clear on what they currently do, so they can reform their processes for the future if necessary.

Data Processors.

Processors have new obligations under GDPR. They must to implement appropriate and reasonable state of the art technical and organizational measures i.e. they must comply with the same security requirements as controllers. They will also be required to support controllers in conducting DPIAs, keeping a register on their data processing activities, supporting the controller for whom he is processing in responding to data subjects' requests and notify Controllers where there has been a breach. Data subjects are entitled to enforce damage claims against a processor if it has acted contrary to its legal obligations or lawful instructions of the controller.

As a result, organisations must have robust data processing contracts in place will need to review existing contracts to ensure the new requirements are incorporated appropriately. Sector specific guidance is expected vv NHS contracts with other NHS organisations which are not enforceable in law.

Data Breach Notification

Organisations need to ensure current processes for detecting, reporting and investigating breaches are robust. The GDPR will require that where individuals are likely to suffer some form of damage or risk to their rights and freedoms as a result of a breach there will be a requirement to notify the ICO within 72 hours of becoming aware of it. Failure to report within the timescale without a 'reasoned justification' may result in a fine on top of the fine for the breach itself. It will also be mandatory to inform the Data Subject of high risk breaches. In large scale losses this may require going to the press.

As part of the IG Toolkit requirements data breaches already need to be documented, investigated and lessons learned. This should be part of the organisations normal governance.

Financial penalties

Fines under the GDPR are significantly increased. There will be a two-tier system. Breaches of privacy by design obligations, the rules relating to processor contracts, record-keeping obligations and processing security requirements will be subject to fines up to €10m or 2% of the organisation's previous annual turnover, whichever is higher. However, breaches of the basic principles for processing, including conditions for consent, infringing data subjects' rights and unlawful transfers to countries outside the European Economic Area will be subject to fines up to €20m or 4% of the organisation's previous annual turnover, whichever is higher.

Subject Access

Currently, the NHS charges £10 for records held electronically and up to £50 for those held manually when responding to Subject Access Requests but this is not allowed for the initial copy under GDPR. Although some charges can be levied e.g. for unfounded or excessive requests or repetitive requests for the same information

There is less time allowed to comply with a subject access request. Information must be provided without delay and at the latest within one month of receipt, although this can be extended by a further 2 months for complex or numerous requests. However, there is now an opportunity for the controller to refuse to act if the request is unfounded or excessive.

As under the DPA the organisation must have an appropriate mechanism to verify the subject's identity and parental responsibility in the case of requests for children's records.

Organisations will need to review their current Subject Access Request procedure to ensure they can comply with the GDPR requirements aand may expect these to increase where they cannot be charged for.

Right to be forgotten

Data subjects have the right to require their data to be erased where it is no longer necessary, where their consent is being relied upon and has been withdrawn, if they object and there is no overriding legal justification. This is unlikely to impact on the NHS as the exceptions applicable are relevant.

Right to Object

Similar to the current right under the DPA (Section 10), the data subject has the right to object to their data being processed. The controller would need to demonstrate legitimate grounds for overriding the objection. Of greater relevance is the new absolute right to object to their data being used for marketing purposes.

This is unlikely to impact on the NHS unless data subject details are used to send out newsletters etc. (direct marketing). Procedures must be put in place to act on any objections received.

Data Portability

Where data is processed under consent or for a contract, subjects must be able to transfer their data from one service provider and to receive data which they have provided to the controller. Where data is electronic, it must be provided in a commonly-used format. Paper or unusual electronic formats mean procedures may need revising.

The GDPR enforces the subjects right to require that their data is erased. Processes will need to be in place to ensure systems allow for the location and (appropriate) deletion of data. Where this requirement is to be met, it will need to be written into contracts and / or Confidentiality Agreements.

Next Steps for CHCs

The implementation of GDPR is the responsibility of the host organisation, therefore, it is recommended that CHCs contact the IG lead for their host organisation to ensure that they are made aware of plans for preparing for GDPR and in particular to ensure they know who the Data Protection Officer will be..

Although it is unlikely that the data being processed by CHCs will fall under the GDPR this is dependent on the discussions with regards to pseudonymised data. It is recommended that the CHCs adopt the approaches described above in relation to:

- Documenting Information that they hold
- Privacy Notices
- Data Protection Impact Assessments for existing and future systems
- Contractual Arrangements with Processors.
- Data Sharing Arrangements

Appendix 1 - Available Guidance

Information Commissioners Office

The Information Commissioners Office are publishing guidance for organisations on how to prepare for the GDPR.

General guidance is available on the ICO website: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/introduction/

and also on https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/

Currently there are two key publications:

- 12 Steps to take now: https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf
- Overview of the GDPR : https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-10.pdf

In addition, the code of practice for communicating with individuals has been developed with the GDPR in mind and can be found: https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf

Information Governance Alliance

The ICO will not be providing sector specific guidance. A national GDPR working group has been established which, together with the Information Governance Alliance (IGA), will help the NHS, social care and partner organisations prepare for GDPR.

The working group has representation from arms' length bodies including CQC, NICE, NHS Improvement, NHS Digital and the NHS European Office, also the Department of Health and Department for Culture Media and Sport who is leading on developing accompanying legislation. There is also representation from the Information Commissioner, the Local Government Association, the chair of a local IG network and the Information Governance Alliance

The working group intend to publish guidance on 12 subject matters:

1. CEO briefing 1: the GDPR and Accountability for Data Protection
2. Data protection accountability and governance
3. Privacy by design and default
4. Implications of the GDPR for Health and Social Care Research
5. Health and Social Care Research: legal basis and safeguards
6. Transparency, consent and subject's rights
7. Consent
8. Pseudonymisation
9. Personal data breaches and notification
10. Profiling and risk stratification

11. GDPR overview
12. What's new and what changes

Publication of the guidance was delayed by purdah but should start to be released soon and will be available from:

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

European Level Guidance

The Article 29 Working Party provide expert advice to member states regarding data protection. It is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. Guidance produces by the working party can be fund here:

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

The WP29 has now adopted guidelines, with FAQs, on the following GDPR topics:

- Data portability
- Data protection officers
- Identifying a controller or processor's lead supervisory authority

They are also planning guidance on:

- Consent
- Transparency
- Profiling
- High risk processing and Data Protection Impact Assessments
- Certification
- Administrative fines
- Breach notification
- Data transfers