HFMA briefing
March 2018

The General Data Protection Regulation (GDPR)

Introduction

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018. This new legislation applies to all organisations collecting and processing personal information and NHS organisations must take action to ensure they are ready.

While many of the requirements of existing data protection legislation are included in the GDPR, governance over the use of personal data has been strengthened. While providing important new rights for individuals, it increases the regulatory requirements on organisations. NHS bodies will need to take steps to ensure that they are compliant with the new legislation and also that they can evidence compliance. Failure to comply with the requirements of the legislation may lead to a fine of up to €20 million or 4% of turnover, whichever is higher.

This briefing aims to raise awareness of the high-level requirements of the new legislation for NHS organisations and to highlight the guidance and support available to ensure that appropriate arrangements are in place. Audit committees may be particularly interested in this briefing.

GDPR requirements

The GDPR is intended to strengthen and unify the protection of personal data. Personal data is anything that can be used to identify a person. The GDPR includes a wider range of identifiers for personal data, reflecting technological changes - such as IP addresses. The Regulation refers to sensitive personal data as a 'special category of personal data', which includes genetic data.

The Regulation refers to the processing of data. Processing data means obtaining, recording, or holding the information or data or carrying out any operation on it. A valid lawful basis is required for processing all personal data. Both those that determine the purpose and means of processing personal data (data controllers) and those responsible for processing personal data on their behalf (data processors) must adhere to the GDPR requirements. Controllers and processors are usually organisations, but can be individuals such as general practitioners, pharmacists and sole traders.

Every organisation will need to be aware of the personal data it holds, where it came from and who it is shared with. Records will be required on all processing activities, setting out its lawful basis and how it complies with data protection principles. Existing policies and procedures will need to be enhanced and organisations must make sure, and demonstrate, that staff are aware of them.

The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. It is the UK's supervisory authority for the GDPR and will monitor the application of it. The ICO *Guide to the General Data Protection Regulation (GDPR)* explains the provisions of the GDPR to help organisations comply with its requirements.

Data protection principles

The GDPR contains data protection principles which cover the main areas of responsibility for organisations:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitations
- integrity and confidentiality
- accountability.

These are largely similar to previous data protection principles. The key changes reflect increased transparency requirements, the purpose of archiving to be in the public interest and the ability to demonstrate compliance with the principles (accountability principle). The accountability principle is a key additional component. This requires organisations to embed a culture of continual monitoring of data processing procedures, ensuring these are clearly documented. The documentation of data processing policies, procedures and operations must be available to the ICO on request.

The rights of individuals over their personal data

The GDPR also provides eight rights for individuals over their personal data:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to object
5. The right to erasure (new)
6. The right to restrict processing
7. The right to data portability (new)
8. Automated decision-making and profiling rights (new)

There are three areas that provide enhanced rights compared to previous legislation. The right to erasure, often referred to as the right to be forgotten, enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Controllers who have passed on this data must also notify others who may be processing it. The new right to data portability means that individuals can view, access and use their data across different services, requiring organisations to maintain the data in a structured and usable format. Making a decision or evaluating an individual solely by automated means without any human involvement is restricted. If it is applied, this type of processing is considered high risk and requires a data impact assessment.

Key changes

In addition to the enhanced principles and rights, there are a number of other key changes in data protection requirements brought in by the GDPR. The changes to the data protection requirements are summarised in **table 1**.

Table 1: The GDPR – key changes to the data protection requirements

Data protection principles	Accountability principle, increased transparency and archiving purposes in the public interest.
Enhanced rights	The GDPR includes the additional right to erasure, data portability and rights in relation to automated decision-making.
Privacy information	The GDPR enhances the disclosures required to individuals, usually covered in a privacy notice, to include items such as the lawful basis for processing the data, retention periods and rights to complain to the ICO.
Data subject access requests (DSAR)	Responses to subject access requests are required within one month (previously 40 days) and in complex cases, it may be possible to extend to an additional 2 months. In most cases no charge can be made.
Consent	Consent must be freely given, informed, specific, unambiguous and verifiable. Consent cannot be inferred and can be withdrawn.
Children	The GDPR provides special protection for children's personal data, particularly in the context of on-line services. If a child is younger than 16, consent from the parent/guardian is required.
Data protection officer (DPO)	A DPO must be in place for all public authorities, those conducting large scale systematic monitoring and those processing special categories (such as health records). The DPO must have knowledge, support and authority.
Data protection impact assessments	A data protection impact assessment (DPIA) is required when using new technologies or for high risk processing.
Privacy by design	For new technology and large-scale processing of special category data, the design of processes and systems must include privacy protection.
Breaches	The GDPR includes processors as a regulated entity. Fines for a breach have increased – there are two tiers of administrative fine which can be imposed dependent on which article has been breached (the first is up to €10 million or 2% of turnover, whichever is higher and the second is €20 million or 4% of turnover, whichever is higher). Breaches must be notified to the ICO without undue delay or within 72 hours, unless the breach is unlikely to be a risk to individuals.

How the regulations apply to the NHS

The GDPR applies to all NHS organisations. The NHS is made up of a large number of organisations that process both staff and patient data, and in many cases they pass this data on to others. The Information Governance Alliance *General data protection regulation (GDPR) guidance* provides a series of advice material to help the NHS, social care and partner organisations prepare for the GDPR. Particular challenges for the NHS are explored below.

NHS systems: Data will be held across a number of locations and systems in NHS organisations, often making it difficult to easily identify data held. It may also be difficult to determine the lawful purpose of data if it has been kept for a number of years. The new right to erasure will also need to be considered, particularly where legacy NHS systems may not be set up to be able to delete data.

Staff: Workforce data is significant for NHS organisations, particularly trusts, with a large number of employees and often a high turnover of staff. The requirements of GDPR can be challenging, particularly for those that do not hold a central log for staff or outsource their HR services.

Consent: In many cases, information flows for the purposes of patient care are currently made on the basis of consent. With the introduction in the GDPR that consent cannot be implied and can be withdrawn, processing on the grounds of consent, and evidencing this, is challenging. However, the GDPR does introduce the processing of provision of health or social care as a special category *(EU regulation GDPR 2016 - article 9.2h*) which should be applied to patient data.

Financial impact: The GDPR will take time and resources to ensure compliance and this is likely to have a financial impact on organisations. Also the loss of income for subject access requests may be significant in some cases.

System working: An increase in system-wide working requires greater data sharing. To ensure that innovation is not hampered, it is important to ensure the right advice and support is sought to ensure appropriate data sharing arrangements are in place.

Charitable funds: The GDPR requirements also apply separately to charitable funds. The charitable fund will need to make its own assessment of what data is held and processes and how it can ensure compliance with the GDPR.

The additional requirements of the GDPR are likely to propose an additional burden on NHS organisations, in the context of already strained resources. Realistic and reasonable plans need to be in place to ensure compliance. Each NHS organisation will need to ensure that they individually assess where they currently are and what they need to do. The attached appendix sets out the top ten actions for NHS organisations to consider. It will be of particular interest to audit committees.

Conclusion

The GDPR provides an important update to existing data protection legislation, recognising today's privacy challenges brought about by changes such as advanced technology and social media. Enhanced requirements do bring with them a greater responsibility for data processors and NHS bodies need to make sure that they meet them. For the GDPR, it is essential that NHS bodies have a clear understanding of how data flows within, and outside of, their organisation and that arrangements are in place to ensure they meet GDPR requirements. As well as this the accountability principle, introduced by the GDPR, makes it essential that NHS organisations can also demonstrate what they are doing to mitigate data protection risks.

Appendix: Top ten actions for NHS organisations

Although many NHS organisations will already have good governance arrangements in place for data protection, all organisations will need to take action to review their current data protection compliance arrangements and determine the next steps. To support organisations to prepare for the GDPR, the ICO's *Guide to the General Data Protection Regulation (GDPR)* includes *Preparing for the GDPR – 12 steps to take now* and *GDPR checklists for data controllers and data processors*. The following top ten actions are prompts that can be used to ensure your organisation is ready for the GDPR.

GDPR actions	Y/N?
Awareness • Are the Board and senior officers aware of the GDPR's requirements? • Have risks been considered and included in the risk register?	
Training • Is there a training plan to ensure all staff are trained effectively and appropriately?	
Information review • Has an information audit been undertaken to identify what personal data is held, the source, where, how it is processed, how long it is retained, when it is passed to third parties and what the legal conditions for data collection and processing are? • Is there a resulting action plan in place to ensure data processing is compliant?	
Policies and procedures • Have policies/procedures been updated to reflect enhanced requirements? • Have measures been put in place to help meet the principles of data protection by design such as data minimisation, pseudonymization and security features?	
New processes or systems • Are arrangements in place to ensure all new processes, systems, and contracts (including employment contracts) consider GDPR requirements at the planning stage? • Are arrangements in place for data protection impact assessments (DPIA)?	
Data protection officer (DPO) • Is a data protection officer in place with seniority to report to the Board? • Do policies require that the DPO is consulted on DPIA issues? • Are arrangements in place to appropriately report data breaches?	
Arrangements for dealing with requests • Have arrangements been made to deal with access requests within one month? • Are arrangements in place to ensure individuals are provided with the enhanced privacy information they should be provided with?	
Documentation • Is there an information asset register in place to evidence compliance? • Is it clear who is responsible for actions in ensuring GDPR compliance? • Is documentation held to evidence policies, procedures and training in place? • Where relevant, are information sharing agreements documented? • Are records of risk assessments and advice given by the DPO maintained?	
Review • Are arrangements in place for ongoing review of compliance i.e. internal audits?	
Charitable funds review • Are separate arrangements in place to ensure charitable funds compliance?	