Information Governance Alliance

CEO Briefing Note

Changes to Data Protection legislation: why this matters TO YOU

Purpose

This briefing note highlights the actions that health organisations and arms' length bodies need to consider to prepare for the EU General Data Protection Regulation (GDPR) which will apply from 25th May 2018. It is expected that the provisions of the GDPR will apply post-Brexit, and for the foreseeable future.

We are letting you know about important changes in the law governing the management and use of patient data in order to give your organisation sufficient time to prepare strategically, and implement the necessary operational changes as advised by your information governance team.

Headline impacts:

- Organisations obliged *to demonstrate that they comply with the new law*
- Significantly increased penalties possible for *any* breach of the Regulation – not just data breaches
- Legal requirement for security breach notification
- Removal of charges, in most cases, for providing copies of records to patients or staff who request them
- Requirement to keep records of data processing activities
- Appointment of Data Protection Officer mandatory for all public authorities
- Data Protection Impact Assessment required for high risk processing
- Data protection issues must be addressed in all information processes
- Specific requirements for transparency and fair processing
- Tighter rules where consent is the basis for processing.

Further guidance

The National GDPR Working Group is leading on the development of guidance to assist organisations in implementing the changes needed to ensure their own compliance. These publications will address areas of the GDPR that impact on health and social care organisations, giving guidance on interpretation and applicability, and a strategic policy steer.

A schedule of planned publications can be found here.[1]

[1] https://digital.nhs.uk/article/1414/General-Data-Protection-Regulation-guidance

Accountability and demonstrating compliance

The GDPR, which was approved in 2016 and comes into force on 25th May 2018 will be directly applicable as law in the UK. It will replace the Directive that is the basis for the UK Data Protection Act 1998, which will be repealed or amended. It is expected that the provisions of the GDPR will remain in force post-Brexit, and for the foreseeable future.

Although in general the principles of data protection remain similar, there is greater focus on evidence-based compliance with specified requirements for transparency, more extensive rights for data subjects and considerably harsher penalties for non-compliance.[2]

The GDPR introduces a principle of *'accountability'*. This requires that organisations must be able to *demonstrate compliance*. The key obligations to support this include:

- the recording of all data processing activities with their lawful justification and data retention periods
- routinely conducting and reviewing data protection impact assessments where processing is likely to pose a high risk to individuals' rights and freedoms
- assessing the need for data protection impact assessment at an early stage, and incorporating data protection measures by default in the design and operation of information systems and processes
- ensuring demonstrable compliance with enhanced requirements for transparency and fair processing, including notification of rights
- ensuring that data subjects' rights are respected
    - (the provision of copies of records free of charge, rights to rectification, erasure, to restrict processing, data portability, to object, and to prevent automated decision making)
- notification of personal data security breaches to the Information Commissioner
- the appointment of a suitably qualified and experienced Data Protection Officer.

Some of these requirements should be established good practice. Organisations that are performing well in their information governance toolkit scores should have a good baseline to work from. However, these legal requirements require organisations to take specified actions, and have evidence to demonstrate that they have done so.

By establishing or adjusting governance arrangements to comply with the GDPR, organisations will be confident not only that they are respecting the law and data subjects' rights but also that they are mitigating risk appropriately and have a defence in the event of a breach. Under the GDPR, the fines available are significantly increased and may be imposed for *any* infringement of the Regulation, not just data security breaches.

[2] There are two tiers: up to 10,000,000 Euros e.g. for security breaches and up to 20,000,000 Euros e.g. for breaches of the principles, data subjects' rights or international transfer restrictions. For more information see https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/

Action plans for compliance

All health organisations should consider the development and implementation of action plans to achieve this demonstrable compliance. Areas to be addressed should include:-

- Appointment of a Data Protection Officer whose job description is compliant with GDPR requirements
- Revision of information governance and related policies to address organisational accountability, Data Protection Officer reporting arrangements within the organisation, and statutory reporting requirements
- Assessment and allocation of resources needed to support the Data Protection Officer role
- Development of an action plan / project plan including but not limited to the following measures:

    - establishing comprehensive records of processing activities (building on existing information asset registers and maps of information flows)
    - review and revision of fair processing information (to provide full disclosure of what personal data is used, for what purpose, who it is shared with and the legal basis for doing so and how long it will be retained)
    - revision of policy and procedures on the introduction of new processes to ensure that
        - the Data Protection Officer is consulted as a matter of routine on the need for data protection impact assessment and other governance matters
        - assurance of compliance is addressed by default in design and implementation of information systems

    - assurance of the compliance of existing business processes and systems
    - review of contracts on renewal / new contracts (including liability for fines in the event of a serious breach) to ensure compliance with GDPR
    - revision to subject access procedures to reflect new timescales and the removal of the fee in most cases
    - development of or revision to procedures to address the other data subjects' rights that are established by the GDPR (highlighted above)
    - collating comprehensive documentation of advice given by the Data Protection Officer, independent risk assessments and management response to provide evidence of compliance with the GDPR.

As the organisation is accountable for compliance, it is recommended that the action plan is formally endorsed by the most senior level of management.

The role of the Data Protection Officer

Appointing a Data Protection Officer as mandated by the GDPR, is essential to achieving effective facilitation across the organisation. The organisation must ensure that the Data Protection Officer has proven expert knowledge of data protection law and practices, and the ability to perform the tasks specified in the GDPR:-

- provision of advice to the organisation on compliance obligations, and when data protection impact assessment is required
- monitoring compliance with the GDPR and organisational policies
- co-operating and liaising with the Information Commissioner
- taking into account information risk when performing the above.

Further requirements of the role are:

- that the Data Protection Officer directly reports to the highest management level of the organisation
- that there is timely involvement of the Data Protection Officer in all data protection issues
- that the Data Protection Officer is supported by the necessary resources and is able to maintain expertise
- that the Data Protection Officer is not pressurised by the organisation as to how to perform his or her tasks, and is protected from disciplinary action when carrying out those tasks
- where the Data Protection Officer performs another role or roles, that there is no conflict of interest.

The role of the Data Protection Officer may be shared by multiple organisations that are 'public authorities' taking into account organisational structure and size, and may be either a member of staff or may fulfil the tasks on the basis of a service contract, provided there is no conflict of interest. The Data Protection Officer should have a good understanding of the organisation's business, and how it processes personal data.

This briefing is not intended to give a specific steer to CEOs on who should be the appointed as the Data Protection Officer. However it is important to consider EU Guidelines that '*[t]he DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case*'[3] Positions that involve the authorising or commissioning of IT or manual records management systems are likely to meet the criteria for determining the purposes and the means of processing.

[3] *Guidelines on Data Protection Officers ('DPOs')* (Article 29 Working Party, 13 December 2016), http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083