General Data Protection Regulation (GDPR)
Frequently Asked Questions (FAQs)
Edition 1

1. **What is the GDPR and when does it become applicable?**
   The GDPR is European Union (EU) legislation that will become directly applicable in Member States (e.g. the UK) on 25 May 2018. It is a regulation by which the European Parliament, the Council of the EU and the European Commission intend to strengthen and unify data protection for all individuals within the EU.

2. **What is the difference between the GDPR and the Data Protection (DP) Bill?**
   The GDPR is EU legislation that will be applicable as law in EU member States (e.g. the UK) from 25 May 2018, irrespective of national legislation.

   The DP Bill will become law when enacted as the Data Protection Act 2017. It will explicitly bring provisions of the GDPR in to UK law and establish continuity of the GDPR in the UK post Brexit. The Act will legislate in areas where the GDPR allows flexibility at national level. It will also introduce legislation on processing for law enforcement purposes (in support of the EU Law Enforcement Directive) and by the intelligence services, and make provision for the Information Commissioner (the UK regulator).

3. **How does this affect current UK law on data protection (DPA 1998)?**
   The DPA 1998 will be completely repealed.

4. **What are the penalties for non-compliance?**
   Fines under the GDPR are up to a maximum of €20 million or 4% of turnover. For health and social care organisations, any fine would be likely to give rise to a loss of public trust, attract media attention and thereby inflict considerable reputational damage. Therefore, it is important organisations ensure their compliance.

5. **How does this affect me?**
   The GDPR strengthens the controls that organisations (data controllers) are required to have in place over the processing of personal data, including pseudonymised personal data.

   Headline impacts are:

   - Appointment of Data Protection Officer (DPO) mandatory for all public authorities

- Organisations obliged to demonstrate that they comply with the new law (the concept of 'accountability').
- Significantly increased penalties possible for any breach of the Regulation – not just data breaches (see above).
- 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.
- Data Protection Impact Assessment required for high risk processing (which includes the large-scale processing of health-related personal data).
- 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.

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.

Organisations should undertake a thorough review of the GDPR requirements, including the helpful and on-going guidance published by the Information Commissioner's Office (ICO), to ensure you are compliant. This is especially important as areas which were good practice are now legal requirements (e.g. the Data Protection Impact Assessment – see below).

Other issues to think about include the information provided to data subjects. Most health and social care organisations provide privacy notices to their data subjects as standard which explains what they use personal data for and why etc. The ICO have published a code of practice on what should be included. The GPDR / DP Bill now requires specific information be provided to a data subject. Articles 12 – 14 of the GPDR set out what will be required.

6. What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a mechanism for identifying, quantifying and mitigating data privacy risks. It is undertaken to ensure appropriate controls are put in place when any new process, system or ways of working involving the use of high risk processing (such as processing "health data") is introduced.

- When undertaking a DPIA, an organisation's designated Data Protection Officer must be consulted. A DPIA should be signed off by

an organisation's Senior Information Risk Owner (SIRO) and the Data Protection Officer (DPO).

- A DPIA has to be completed before any new process, system or way of working goes live (i.e. at the business planning stage of a project) where it involves high risk processing.

- The completion of a DPIA will help to minimise the chance that any new process, system or way of working will present a high risk to the rights of individuals through a failure to comply with the GDPR (or new DPA).

7. **What/who is the DPO?**
   The GDPR requires all public authorities to have a DPO. Their role is to inform and advise their organisation(s) about all issues in relation to GDPR compliance.

   The DPO will also be responsible for monitoring the organisation(s) compliance with the GDPR.

   It is important to note that data processors that process personal data on behalf of health or social care organisations must appoint a DPO where they either:

   a. process special categories data on a large scale OR
   b. perform regular or systematic monitoring of data subjects

   The DPO reports directly to an organisation's highest management level and may not be disciplined or dismissed for carrying out their tasks as a DPO. It is envisaged that the DPO will be supported by the organisation's Information Governance (IG) and/or Information Communication Team (ICT).

8. **Who can be a DPO?**
   Organisations must ensure that the DPO role is independent, free from conflict of interest. DPOs 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. A DPO team with a nominated contact for each organisation is an acceptable approach.

   There are specific roles that the DPO cannot perform in conjunction with this new role. As a result it is important to consider EU Guidelines that state:-

'[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'

and further:

'As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing'

9. How can I prepare for GDPR?

The ICO have published and will continue to publish guidance to assist organisations in understanding how to comply with data protection reform (i.e. GDPR and thee new DPA). The Information Governance Alliance (IGA) will also publish GDPR guidance for the health and social care system to support that published by the ICO.

Please monitor these websites or sign up to their newsletters.

10. What guidance does the ICO intend to publish

The ICO has already started to publish useful information and will continue to do so.

11. What guidance does the IGA intend to publish?

The IGA is currently looking at drafting guidance across the following topics:-

- CEO briefing: the GDPR and Accountability for Data Protection
- Data protection accountability and implementation priorities
- Privacy by design and default
- Transparency and subjects' rights
- Consent
- Pseudonymisation
- Personal data breaches and notification
- Profiling and risk stratification
- GDPR overview
- What's New
- GP Practice / primary care suite
- The data protection officer
- Lawful processing
- Social care awareness guidance
- FAQs

12. **What guidance is intended for publication by the IGA and when?**
    The original intention was to publish a set of guidance across a series of timeframes. However, we have incurred delays and we acknowledge the need to consider not only the Article 29 Working Party guidance which will inform guidance from the ICO but also the DP Bill. This, upon approval may require changes which could affect advice provided. The IGA are working hard to try and provide as much advice as it can in the circumstances.

    The list below gives an idea of the anticipated, timeframe for publication. Please note this is subject to change. Where changed, we will update our website.

    - Published:-
        - CEO briefing: the GDPR and Accountability for Data Protection
    - December 2018
        - FAQs
    - January – February 2018:-
        - Transparency and subjects' rights
        - Social care awareness guidance
        - Data protection accountability and implementation priorities
        - Consent
        - Pseudonymisation
        - The data protection officer
        - What's New
        - Lawful processing
    - March – April 2018:-
        - Privacy by design and default
        - Personal data breaches and notification
        - Profiling and risk stratification
        - GDPR overview
        - GP Practice / primary care suite

13. **What about Health Research guidance**
    The Health Research Authority (HRA) intends to publish guidance – please check their website for further details.

14. **For requests under the Access to Health Records 1990 for access to records of the deceased, will the 40 calendar days and the application fee up to £50 still apply when GDPR is in place?**
    Under this legislation in particular Section 3(4)(a); it refers to the “prescribed” fee in relation to DPA but does not relate the timeframe to the DPA. Therefore, it is considered at present that the timeframe under this Act

remains at 40 calendar days but the fee matches that of the DPA. This will be £0 in the GDPR / DPA 2 (unless exceptional circumstances apply).

15. **Do GP practices / federations need their own DPO given some can have over 30,000 patients?**
    Please refer to Q7 and Q8.