Social care organisations hold a significant amount of personal information relating to individuals, whether they be employees, people who need care and support or other customers or suppliers. A proportion of that data is likely to constitute sensitive personal data or “special categories of data” (including for example, medical records, religious beliefs or ethnic origin).

All organisations that process personal data are required to comply with the Data Protection Act 1998 (DPA) and, from 25 May 2018, the General Data Protection Regulation (GDPR). Penalties for failure to comply, including fines, are significant. If GDPR isn’t already on your organisation’s agenda, now is the time to act.

Get Data Protection Ready

The GDPR extends current requirements set out in the Data Protection Act 1998 and places new obligations on organisations that process personal data and special categories of data. These include, amongst others:

1. more stringent requirements around consent, particularly if special categories of data are involved;

2. the right to be forgotten;

3. taking an approach to projects that promotes privacy and data protection compliance from the start and using privacy impact assessments to identify and reduce risk;

4. a modified subject access request procedure that favours the individual;

5. if there is a breach of GDPR there are new, stricter requirements to notify the Information Commissioner’s Office and the affected data subjects; and

6. expanded territorial reach – a non-EU company could be subject to the same sanctions as EU companies.

What are the key implications for organisations in the health and social care sector?

Social care organisations will be affected by the majority of changes introduced by GDPR. The DPA already requires social care employers to be compliant and robust due to the nature of the data frequently being processed. Where this is in place, it will facilitate compliance with GDPR.

Some of the changes that will be introduced by GDPR are advantageous to social care organisations and some will create additional obligations or administrative burden. A few examples are set out below, but the list is by no means exhaustive:

- **Subject Access Requests (SAR)** – requests from current and former employees, as well as people who need care and support, for sight of all data held about them are relatively common in the social care sector. GDPR removes the £10 fee payable to make a request and decreases the timescales for complying with a request from 42 days to 1 month. Removal of the £10 fee may result in an increase in the number of SARs placed, simply because an administrative obstacle has been removed. Organisations should ensure they have the appropriate policies and procedures in place to collate the relevant data and respond within the new timescales.

- **Impact on Children** – GDPR requires greater information to be provided to data subjects about the personal data that is being processed. This is particularly challenging if the data subject is a child, in which case it is particularly important to ensure the information is concise, clear and easy to understand. Social care organisations should consider whether it is appropriate to have separate template notices and policies for adults and for children.

- **Processing of Personal Data** – one of a number of grounds must be met for personal data to be processed by an organisation. “Processing” is widely defined in both the DPA and GDPR and includes simply holding or storing the data. At the point an organisation collects the data, it will be processing it, whether or not...
Social care sector organisations should already be in the process of considering the potential impact of GDPR on their policies, procedures and systems. Budget and resource will need to be allocated to GDPR compliance, bearing in mind that GDPR encourages each organisation to adopt what it considers an appropriate and proportionate response to GDPR compliance, and evidence that response in writing. NHS Digital has issued and updated guidance (available online) around record management and data retention which, where relevant, should be reviewed.

Addressing compliance with GDPR can seem daunting, but it doesn’t need to be. Although it potentially requires a significant level of time and resource dedicated to it by the business, it is possible to break down GDPR compliance into bite size chunks on a risk analysis basis.

There is up to date guidance from the Information Commissioner’s Office available online. Clarion also have a series of blogs which help to explain the impact of GDPR. If you would like any further information or have any questions about the changes that GDPR will introduce, please contact Clarion’s Commercial, IT and Privacy team.