MILLS & REEVE

Processing of Personal Health Data under the EU General Data Protection Regulations

The EUGDPR are designed to bring the data processing law up to date with a society where the vast majority of personal data exists digitally. For those of us familiar with the old Data Protection Act the big question is, what do I need to do differently now?

Hang on - doesn't Brexit mean we don't need to worry about this?

True, the GDPR is EU law. But irrespective of how Brexit pans out, we expect the principles it embodies to come into UK law between now and May 2018 (when they would have effect under the EU regime). Indeed the ICO advises all health and care providers to prepare for the new rules promptly.

What's changed from the DPA regime?

As now, before processing, we need to identify the category of data and then ensure we meet the lawful conditions for processing. Most requirements for lawful processing are similar to the DPA regime and will be familiar. But there are some subtle and important changes. This briefing tells you what you need to know.

Personal data

This category and the conditions for lawful processing are largely (but not entirely) unchanged from the DPA regime.

Personal data | Lawful processing conditions

- Consent of the individual
- Compliance of a legal obligation
- Performance of a contract with the data subject (or steps to enter into a such a contract)
- To protect vital interests of a data subject or another person
- Performance of a task carried out in the public interest or in exercise of official authority vested in the controller

An important change: public bodies (including hospitals and other care providers) can no longer use the "legitimate interests" basis to justify processing. It can, however, be used by health and care organisations in the independent sector.

Health and care bodies will have to make sure one of the conditions (above) apply and hence define the lawful basis for all processing of all personal information. This includes the exchange of information between public and independent organisations. It's important you are clear about which condition applies and you record this. The UK should follow this with guidance or even regulations specifically for health bodies. The mechanism and timescale for this depends on how EU exit pans out and how the GDPR enters UK law.

MILLS & REEVE

Special category data

What is it and what it includes

Special Category Data is the new term for what was sensitive personal data under the DPA. As with the DPA, processing of this data is only allowed in clearly defined circumstances.

It includes health and care data, and there is a specific processing condition for provision and management of health and care services. This will be useful for commissioners and providers.

SCD specifically includes genetic and biometric data – where processed for the purposes of providing a unique identifier for an individual. Information relating to criminal convictions and offences are now dealt with under separate provisions.

Special category data | Lawful processing conditions

- Explicit consent of the individual
- Necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- To protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- Carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Relates to personal data manifestly made public by the data subject
- Necessary for the establishment, exercise or defence of legal claims or where the courts are acting in their judicial capacity
- Necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- Necessary for reasons of public interest in the areas of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes

Consent and processing of healthcare data

This applies across Personal and Special Category Data.

- Consent must be explicit and requires clear affirmative action. It cannot be implied. Silence, pre-ticked boxes or inactivity is not enough.
- Consent must be verifiable. A full record must be kept.
- People can withdraw consent at any time.
- You can rely on consent obtained under the DPA 1998 if it meets the standard of the GDPR. You will need to check this or (perhaps best) get fresh consent.

And if you don't have consent...

If you cannot rely on consent then you will need to use on one of the conditions – otherwise processing must stop.

In the health and care sector, the likely relevant conditions for processing are:

- Protecting a person's vital interests (eg, life and death of the patient).
- Substantial public interest (eg ,a criminal investigation to which it is germane).
- The provision of health and care or treatment and the management of health and care systems (eg, commissioning).
- Public interest in the areas of public health (eg, managing an outbreak such as Legionnaires).
- Archiving in public interest, scientific and historical research (eg, old medical records).

Who may process health data?

The EUGDPR extends the scope of "professionals" entitled to process health data. For example, this includes processing by professionals for the purpose of:

- Preventative occupational medicine
- Medical diagnosis
- Provision of health and social care/treatment
- Management of health and social care systems

Provided the individual is managed by someone who has a professional obligation of secrecy/confidentiality under UK law or is regulated by rules of a national competent body (eg, GMC, NMC).

MILLS & REEVE

For more information

EU GDPR - the Regulations
The ICO Data Protection reform page
Health & Care Update - information governance blogs

Richard Sykes
Partner
+44(0)121 456 8486
richard.sykes@mills-reeve.com

Jill Weston
Principal Associate
+44(0)121 456 8450
jill.weston@mills-reeve.com

Stuart Knowles
Consultant Solicitor
+44(0)121 456 8461
stuart.knowles@mills-reeve.com