National Data Opt-out: Factsheet 6 – How it fits with data protection legislation

This is one of a series of factsheets about data uses and the national data opt-out

Published 25 May 2018

Factsheet 6 – How it fits with data protection legislation

Purpose

This factsheet provides information about how the national data opt-out fits with data protection legislation and the General Data Protection Regulation.

The national data opt-out (offered to the public as '*Your Data Matters to the NHS*')

The national data opt-out allows a patient to choose that they do not want their **confidential patient information** to be used for purposes beyond their individual care and treatment.

Changes to data protection legislation

The EU General Data Protection Regulation (GDPR) introduced on 25 May 2018 as law in the UK replaces the Directive that is the basis for the UK Data Protection Act 1998, which will be repealed or amended to put in place a new or updated Data Protection Act (DPA) to enact the GDPR.

Although in general the principles of data protection remain the same as previous legislation, there is a greater focus on evidence-based compliance with specified requirements for transparency, more extensive rights for data subjects and considerably harsher penalties for non-compliance.

Further information and guidance about GDPR for health and care organisations is provided by the Information Governance Alliance (IGA) and the Information Commissioner's Office (ICO).

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The national data opt-out is Government policy that sits alongside and is not replaced or changed by GDPR and data protection legislation. It is in addition to the data subject rights required by law.

The following provides more information on key areas where there may be confusion between the policy offer of a national data opt-out and legal requirements under GDPR and data protection legislation.

Legal bases

GDPR and data protection legislation require that processing of personal data is fair, lawful and transparent.

To be lawful in the UK the Common Law Duty of Confidentiality (CLDC) must be satisfied in addition to the DPA.

Under GDPR this means that for recording and processing health and care data:

- an Article 6 condition[1] needs to be satisfied (for personal data); **and**
- an Article 9 condition[2] needs to be satisfied (as health data is a special category of data)

and, to respect confidentiality under CLDC, there is:

- consent from a patient for the use of their data under common law; **or**
- there is another legal basis which enables the CLDC to be set aside (i.e. a mandatory legal requirement, Section 251 (NHS Act 2006) support, or an overriding public interest)

[1] http://www.privacy-regulation.eu/en/article-6-lawfulness-of-processing-GDPR.htm
[2] http://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm

It is important to recognise that if a patient does not have a national data opt-out recorded, it does not mean their confidential patient information can be used for purposes beyond individual care and there must still be a lawful basis to meet the DPA and CLDC to process such information.

Further information about the legal protections and lawful bases for data use can be found in Factsheet 1B – "Types of data used and legal protection in place", and Factsheet 2 – "When it applies".

Consent

'Consent' to meet the CLDC requirements should not be confused with consent to processing under GDPR and data protection legislation.

Further detail on the CLDC consent requirements can be found in Factsheet 1B – "Types of data used and legal protection in place".

The ICO has advised that using consent as the lawful basis for the recording and processing of data under GDPR should be avoided by public authorities, such as health and care providers. This is because it is unlikely to be able to meet the strict requirements around consent, most notably it cannot be considered freely given if access to health and care services are dependent on it. The ICO recommends that another lawful basis is used, GDPR Articles 6 and 9 both provide appropriate legal bases under which to record and process health and care data. The IGA has provided further guidance on this for health and care organisations.

It is still possible to use consent to satisfy the CLDC and in such cases there is no need to change consent practices that already meet the CLDC requirements.

The GDPR 'right to object'

The right to object is a legal right, whereas the national data opt-out is a policy offer that the Government has agreed should be provided to patients and the public in addition to their legal rights.

The national data opt-out has a different effect on the use of confidential patient information to the right to object, therefore they are treated separately, and data controllers must have arrangements to implement both.

Under GDPR the patient has the right to object to "processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)". The right to object will only apply to data processing by the organisation that the patient raises the request with, and the data controller for that organisation will consider the request and decide upon the action to take.

The national data opt-out differs as the patient is responsible for setting the opt-out, it only needs to be set once and will then be applied by all health and care organisations, and the patient does not need to provide information to support their choice to set a national data opt-out.

For more information on the timescales for national data opt-outs to be applied across health and care organisations see Factsheet 4 – "How it is applied".

Where a patient has a national data opt-out in place, an organisation that receives a request from a patient to exercise their right to object will need to follow their own established processes to consider the patient's request.

Transparency and Privacy Notices

The GDPR strengthens the requirements on data controllers to provide clear and concise information to data subjects to be fairly and lawfully processing information. Essentially this is about being clear with patients and the public about what data is collected and how it is processed.

This information should be described accurately and clearly within the organisation's Privacy Notice (or 'Fair Processing' material) and made available to patients.

The introduction of the national data opt-out is intended to support this duty of transparency that all health and care organisations need to meet, by providing additional information for public and patients on how their data may be used across the health and care system for purposes beyond their individual care and treatment and the choice and control they have over this.

The 'right to object' under GDPR must be clearly communicated as part of a Privacy Notice and it is advised that the offer of the national data opt-out is also made clear within the Privacy Notice. This will enable patients to understand the options available to them about use of their confidential patient information, and to make an informed decision as to whether they want to request a 'right to object' with a particular organisation and/or to set a national data opt-out, which may be more appropriate to address the concerns they have over the use of their data e.g. as it has a wider application.

Guidance and information about the national data opt-out offer which can be included in organisations' Privacy Notices can be found at: https://digital.nhs.uk/national-data-opt-out.

Anonymisation guidance

The Information Commissioner's Office (ICO)'s anonymisation code of practice provides good practice advice for all organisations that need to convert personal data into a form in which individuals are no longer identifiable. It covers a range of types of anonymised data from aggregate data through to de-identified individual-level data and sets out how this can meet the legal tests required under the DPA when considering the risk of identification of an individual. The national data opt-out does not apply to data which is anonymised in line with the ICO code.

Organisations need be aware that the ICO will be reviewing their code of practice after May 2018 when the GDPR has come into force and the new data protection legislation is expected to be in place. Once new guidance is issued by the ICO organisations will need to make sure they are compliant with the latest guidance on anonymisation before determining that national data opt-outs do not need to be applied.

Further information about anonymisation can be found in Factsheet 2 – "When it applies".