Care.data

Legal guidance

For GPs and practice staff in pathfinder practices

Legal guidance

Contents

1. Legal responsibilities in relation to the care.data programme

There is some confusion about general practices' legal obligations in relation to the care.data programme and requests were made to explain this clearly. This guidance is intended to provide clarification of the care.data programme's view of the legal position so that general practices feel supported in ensuring that they meet their legal responsibilities.

2. Scope of this guidance

The guidance focuses on the law in relation to providing data to the Health and Social Care Information Centre (HSCIC) for the care.data programme where the data is being required under the Health and Social Care Act 2012.

It does not cover other requests for confidential data by the HSCIC for which there must be a legal basis or consent. Also it does not cover other local and national data flows, e.g. to the Data Services for Commissioners Regional Offices (DSCROs), for local commissioning purposes. For advice on other local and national data flows practices should speak to their Caldicott Guardian[1].

3. Ensuring compliance with the Health and Social Care Act 2012

By providing information for the care.data programme to the Health and Social Care Information Centre, general practices are complying with the Health and Social Care Act 2012

Under section 259 of the Health and Social Care Act 2012, general practices are required to provide information to the HSCIC when the HSCIC considers this is necessary or expedient to meet a 'direction' or 'mandatory request'. In this case NHS England will direct the HSCIC to collect the data for the care.data programme[2].

Section 259(5) of the Health and Social Care Act 2012 states:

> (5) *A requirement under subsection (1)(a) must be complied with by providing the information to the Information Centre in such form and manner, and within such period, as the Centre may specify.*

General practices must comply with the Health and Social Care Act 2012. It is a legal requirement.

[1] The BMA and GMC also provide advice on confidentiality on their websites.

[2] Directions will be issued once the National Data Guardian, Dame Fiona Caldicott, has advised the Secretary of State that she is satisfied with the proposals and safeguards.

4. Ensuring compliance with the common law

General practices will not breach the common law when providing data for the care.data programme. Disclosures covered by section 259 of the Health and Social Care Act are not in breach of the common law duty of confidentiality.

Common law is case law determined by the Courts. Common law has established that patients provide information to doctors in confidence, therefore the information is subject to a legal duty of confidentiality. This means that the information must not normally be disclosed without the consent of the patient.

There are some limited occasions when this can be overridden, for example, where the law requires the disclosure of information. As set out above, the Health and Social Care Act 2012 places a requirement on general practices to disclose information to the HSCIC. Section 259(10) of the Act says that disclosures do not breach the duty of confidence.

General practices do not therefore need to seek patient consent for disclosures for the care.data programme.

5. Ensuring compliance with the Data Protection Act 1998

Under the Data Protection Act 1998, general practices are required to tell their patients that they have a legal duty to provide information to the HSCIC for the care.data programme.

The Data Protection Act requires data controllers to ensure personal data is processed fairly; this means that individuals are informed about how information that could identify them is handled, including the purposes for which it will be used and who is responsible for looking after the data (see section 7.2 for further information).

General practices are data controllers for their patient records and therefore are responsible for ensuring that information is readily available to patients about what the general practice will do with a patient's information and whom it may be shared with. This includes the use of data for direct care and for purposes beyond direct care.

As set out above, general practices also have a legal duty, under the Health and Social Care Act 2012[3], to provide the HSCIC with certain patient information for the care.data programme. It is the view of the Information Commissioner's Office that the requirement to make patients aware of the use of their data remains[4] and [5].

[3] Once directions have been issued as set out in section 3.

[4] The Information Commissioner's Office view is that compliance with the first principle of the DPA, to process personal data fairly, is not 'inconsistent' with the disclosure to the HSCIC i.e. providing fair processing information to

In relation to the care.data programme, this means that general practices should take reasonable steps, so far as practicable, to ensure that patients are made aware of, and understand:

i. the requirement for data from their medical records to be provided to the HSCIC
ii. how and when their practice will disclose it
iii. that they can opt out of their GP data being used for purposes beyond direct care and how they may do so
iv. where to find out more information about why the information is being extracted, what it will be used for and how it will be processed by HSCIC.

General practices should actively provide the information described above to all registered patients including those who do not regularly visit the surgery.

The methods used to achieve fair processing are a matter for each individual general practice, as they will know what communications methods work best with their group of patients. However, the care.data programme will be working with pathfinder practices with different demographics, to explore the support and materials general practices require to help them best meet their fair processing responsibilities so this can inform national roll out. This is likely to include several forms of communication to achieve maximum coverage.

Whilst it is the general practice's responsibility to provide their patients with this high level information, the HSCIC and NHS England also have fair processing responsibilities. The HSCIC and NHS England will produce the detailed fair processing information necessary and sufficient to enable the patient to opt out and have their questions answered. This information is also most easily communicated to patients through general practices as well as through the HSCIC and NHS England's web sites and other channels so that patients and their doctors are best informed in the most convenient way. The care.data programme has worked with pathfinder practices to produce a range of materials to meet this requirement.

For more information on how the care.data programme is supporting general practices to meet their fair processing responsibilities, please see section 3 of the Information Governance guide, which covers the Fair Processing Mailing Exercise.

6. Further information:

The Information Commissioner's Office Guide to data protection:
https://ico.org.uk/for-organisations/guide-to-data-protection/

patients does not affect the statutory disclosure (Further information about when exemptions apply is at: http://ico.org.uk/for_organisations/data_protection/the_guide/exemptions

[5] The GMC guidance on confidentiality also provide information about disclosures required by the law: http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_17_23_disclosures_required_by_law.asp

'Looking after your health and care information ' HSCIC webpages
http://www.hscic.gov.uk/patientconf

General Medical Council (GMC) guidance on confidentiality:
http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp

British Medical Association Confidentiality Toolkit:
http://bma.org.uk/practical-support-at-work/ethics/confidentiality-tool-kit

7. Frequently Asked Questions in relation to legal responsibilities:

7.1 Who is the data controller for care.data?

Under the Data Protection Act 1998, the patient (who the data is about) is the data subject.

The general practice is, and continues to be, the data controller for the sensitive personal information it holds and processes about a patient (the data subject).

Once data is collected, the HSCIC and NHS England become joint data controllers for the data held by the HSCIC as part of the care.data programme:

- NHS England, because it is the organisation determining the purpose for the processing of the data (i.e. the data will be processed to meet the aims of the care.data programme); and
- The HSCIC, because the data is held on computers which the HSCIC is responsible for and it determines the manner of the processing of the data (i.e. the data will be processed in a specific way to meet the aims of the care.data programme).

7.2 How can I be sure I am compliant with the Data Protection Act 1998?

For the care.data programme, general practices are exempt from a number of the Data Protection Act principles because the disclosure is required by an enactment. This is set out in section 35 of the Data Protection Act 1998[6].

In relation to the Data Protection Act principles, the first principle[7] is met because:

1. The processing has a lawful basis under the Health and Social Care Act (it will not breach confidentiality).
2. The data can be viewed as being obtained fairly because it has been required by enactment[8] . Note that this does not remove the requirement for general practices to

[6] Section 35 - Disdosures required by law or made in connection with legal proceedings etc. (see http://www.legislation.gov.uk/ukpga/1998/29/section/35).
[7] The first principle states that 'Personal data shall be processed fairly and lawfully'
[8] Schedule 1, Part II para 2(b)

inform patients that the data is to be used for other purposes other than that which it was collected or the HSCIC/NHS England's requirements for fair processing.

When general practices disclose information to the HSCIC, section 35 of the Data Protection Act 1998 applies which provides an exemption from the second, third[9], fourth and fifth data protection principles[10]. Measures have been put in place to ensure that the sixth[11], seventh[12] and eighth[13] Data Protection Act principles are complied with[14].

Overall, this should mean that the Data Protection Act requirements will be met for obtaining the data provided patients are informed of this use of information about them. The Data Protection Act will not restrict or prevent disclosure to the HSCIC under the Health and Social Care Act 2012.

It is important to note that these exemptions apply when providing information for the care.data programme because the disclosure is required by an enactment. The exemptions may not apply to other local and national data flows of data.

7.3 Will I breach any legislation if I apply opt-out codes to all my patients?

Yes. General practices that bulk opt out would be in breach of the requirement under section 259 of the Health and Social Care Act 2012 to provide the HSCIC with the information it requires. This is because:

- There is a clear implication in section 259 that the information supplied should not be deliberately inaccurate. Bulk opt-outs deliberately code patients as objecting to use of their data when they have not done so.
- Practices would not be supplying the required data to HSCIC about patients who had not opted out. This is because they will be coded as having opted out therefore the data will not be supplied.

In addition, all General Medical Services, Personal Medical Services and Alternative Provider Medical Services contracts with GPs include a requirement for them to comply with relevant legislation.

---

[9] Although GP practices are exempt from the third principle that personal data shall be adequate, relevant and not excessive there is a requirement in the Health and Social Care Act 2012 that information must be 'necessary or expedient'.

[10] The data protection principles are set out here: http://www.legislation.gov.uk/ukpga/1998/29/schedule/1

[11] The 6th principle states 'Personal data shall be processed in accordance with the rights of data subjects under this Act'.

[12] The 7th principle states: 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'. All of the HSCIC's systems and services are designed and operated in accordance with multiple international security standards and best practices.

[13] The 8th principle states: Personal data shall not be transferred to a country or territory outside the European Economic Area...'. The data is being provided by GP practices to the HSCIC, which is within the EEA. It is the responsibility of the HSCIC/NHSE to provide information about onward disdosure from the HSCIC

[14] Further information about the DPA principles are at: https://ico.org.uk/for_organisations/data_protection/the_guide/the_principles

7.4 What action would the Information Commissioner's Office take if a patient complained that they were not aware of the plans to collect GP data for care.data?

If a patient thought they had not been informed of the changes and therefore had been unable to opt out, the Information Commissioner's Office would look into the matter. The efforts made by the general practice to communicate the changes would be taken into consideration. The Information Commissioner's Office would also consider the efforts made by the HSCIC and NHS England in ensuring the fair processing of the actual extraction and processing of the data.

The outcome of any investigation would depend upon the circumstances of the specific case. If it is discovered that the individual/s have not been informed about data sharing for purposes other than direct care, the general practice is likely to be asked to immediately provide the patient with the relevant information and, if required, add the appropriate opt out code to their record. Any enforcement action taken would be in line with the Information Commissioner's Office policy, which is risk based and takes into account the seriousness of the matter and the effect on the individual[15].

7.5 Why can't NHS England indemnify general practices against a patient complaining/suing a general practice that their data had been extracted for the care.data programme without them being aware?

General practices as data controllers are responsible for meeting the fair processing requirements of the Data Protection Act 1998. It is not appropriate for NHS England to indemnify other organisations against breaching legislation that applies to them.

However, the care.data programme will provide materials and advice to support general practices. These materials have been reviewed at a national level by a range of stakeholders including by the Information Commissioner's Office and the Medical Defence Organisations. In addition, no data will be extracted from general practices as part of the care.data programme until the National Data Guardian, Dame Fiona Caldicott, has advised the Secretary of State that she is satisfied with the proposals and safeguards.

The programme has engaged with the Medical Defence Organisations on a regular basis. They have been sent the public facing and GP materials for comment as part of the co-production process. The Medical Protection Society has a statement on their website about care.data which is available at:

http://www.medicalprotection.org/uk/care.data

This includes the following:

[15] Further information is at: https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection-and-electronic-marketing/

“A GP’s principal responsibility concerning the care.data programme relates to the fair processing of information. Practices must ensure that they engage with the process and follow any guidance issued by NHS England as this will put them in the best position in the event that a complaint is raised. If you follow NHS guidance in engaging with the process we believe it is unlikely that a complaint or legal action would be successful”.