Department of Health & Social Care

From the Lord Bethell
Parliamentary Under Secretary of State for Innovation (Lords)

39 Victoria Street
London
SW1H 0EU
Tel: 020 7210 4850

By email to: Lord Stirrup

22 June 2021

Dear Lord Stirrup

Thank you for your question in the House of Lords on the 8 June regarding the new GP Data for Planning and Research system:

> "My Lords, we urgently need better flows of clinical data between different parts of the NHS, but the public are understandably anxious, given the well-publicised data leaks and thefts of recent years, and particularly given that the proposed scheme is not limited to the NHS but includes external third-party commercial enterprises. Why have the Government done so poorly at explaining to the public the need for such information flows and the health benefits that they bring? Why have they not, at least in the first instance, constrained the sharing of data more narrowly, in order to build up the necessary degree of public confidence?"

As I said in the opening remarks of my response in the House, data saves lives and is vital for the effective development and operation of the NHS. The health service is rich with data which can provide us with life-saving insights. For years it has been used to help us better understand and develop cures for serious illnesses, such as heart disease, diabetes, and cancer, and it has been crucial in our response to the pandemic over the past year.

Data enables services to be planned and targeted where they are most needed, new treatments to be developed and patient care to be assessed and improved. Data from General Practice is already used today and has been used for many years to support multiple operational and research needs.

The new GP Data for Planning and Research system will replace the current GP Extraction Service (GPES), improving and simplifying processes, reducing the burden on GPs, improving data security, enabling greater transparency for patients and reducing the amount of patient data being shared between organisations.

We are committed to ensuring that this data is held and used safely, adhering to the UK's high data protection standards such as through the UK GDPR and the Data Protection Act 2018. I attach an overview of the UK's data protection regime, which highlights the measures in place to ensure data is adequately protected.

I hope this list of all the various restraints and restrictions on our use of data reassures you that there is a strong legal and regulatory framework for the handling of patient data. This letter will be sent to others who spoke in the debate and a copy will be placed in the House of Lords library.

With my very best wishes,

LORD BETHELL

ANNEX A

Data Protection Legislation

1. All use of personal data in the UK is subject to the following data protection legislation:

    - UK General Data Protection Regulation (UK GDPR)[1]
    - Data Protection Act 2018 (DPA)[2]

2. The UK GDPR establishes the basis for sharing personal data (that is data which directly or indirectly identifies a living person). The DPA puts those safeguards into UK Law.

3. The legislation provides several key protections and safeguards for the use of an individual's data as set out below.

Principles for sharing data

4. Sharing of personal data in the UK has to follow strict rules and must follow the seven key data protection principles set out in the UK GDPR[3]. These provide that personal data must be:

    - used fairly, lawfully and transparently.
    - used for specified, explicit and legitimate purposes.
    - used in a way that is adequate, relevant and limited to only what is necessary.
    - accurate and, where necessary, kept up to date.
    - kept for no longer than is necessary.
    - handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.
    - used responsibly ensuring compliance with the principles of the UK GDPR.

Lawful basis[4]

5. The UK GDPR and the DPA set out the ways in which personal data can be lawfully processed. All processing of personal data must be on the basis of at least one of the following:

---

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

[2] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[3] More information on the principles can be found on the ICO website

[4] More information on the legal basis for processing data can be found here

- consent: the individual has given clear consent for you to process their personal data for a specific purpose;
- contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract;
- legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations);
- vital interests: the processing is necessary to protect someone's life;
- public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law;
- legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

6. Under the UK GDPR, health data is defined as special category data[5] (that is data that requires additional protections due to its sensitivity). For this type of data to be processed a further condition must be met in addition to one of the lawful bases set out above. These conditions could be that the processing is:

    - with the explicit consent of the data subject.
    - necessary to obligations in relation to employment, social security and social protection (if authorised by law).
    - necessary to protect a person's vital interests.
    - by not-for-profit bodies in relation to members/former members/regular contacts in connection with a body's purposes.
    - of data made public by the data subject.
    - necessary for legal claims or judicial acts.
    - for reasons of substantial public interest (with a basis in law).
    - for health or social care purposes (with a basis in law).
    - for public health purposes (with a basis in law).
    - necessary for archiving, research and statistics (with a basis in law).

<u>Individuals' Rights</u>

7. Data protection legislation sets out rights which individuals have over the use of their data. These individual rights are:

    - the right to be informed.

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

- the right of access.
- the right to rectification.
- the right to erasure or restrict processing.
- the right not to be subject to automated decision-making and profiling.
- the right to object.
- the right to data portability.

8. These rights are not absolute and there are a number of exceptions, such as protection of the individual or the public. More information on individuals' rights can be found on the ICO website[6].

9. Data legislation also provides for the enforcement of these rights through a regulatory body. In the UK this is the Information Commissioner and more detail on this can be found in the section on independent oversight below.

Common Law

10. Alongside data protection legislation, the common law duty of confidentiality also applies to the use of confidential patient information.

11. The general position is that if information is given in circumstances where a duty of confidence applies, that information cannot normally be disclosed without the consent of the individual.

12. The three circumstances where disclosure of confidential patient information is permitted are:

    - where the individual to whom the information relates has consented;
    - where disclosure is necessary to safeguard the individual, or others, or is in the public interest;
    - where there is a statutory basis for disclosing the information or a legal duty (such as a court order) to do so.

Human Rights Law

13. Article 8 of the European Convention on Human Rights (ECHR) requires public bodies to respect the private life of an individual, including protecting any information held about them. However, this right is not absolute and can be interfered with where that interference is provided for by law and is, for example, necessary to protect public safety, health or the rights and freedoms of others. Public bodies must be able to justify storing or processing of any personal data and the principles of necessity

[6]https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

and proportionality when assessing such rights, are an important consideration. Public bodies have a duty to:

- take active steps to prevent breaches.
- deter conduct that would lead to a breach.
- respond to breaches.
- provide information to service users about their rights and the risks to those rights.

Independent Oversight and Advice

14. In the UK, the Information Commissioner upholds information rights as the independent regulator dealing with the Data Protection Act 2018 and the General Data Protection Regulation. The Information Commissioner investigates complaints of breaches of data law and can issue fines where complaints are upheld.

15. The Information Commissioner also provides guidance on the operation of the DPA and UK GDPR which can be found on its website[7].

16. In England, the National Data Guardian for Health and Social Care is a statutory role established to advise and challenge the health and care system to help ensure that individuals' confidential patient information is safeguarded securely and used properly.

17. The former National Data Guardian, Dame Fiona Caldicott, established the Caldicott Principles which inform the use of confidential patient information in the health and care system[8]. These principles are:

- Justify the purpose(s) for using confidential information.
- Use confidential information only when it is necessary.
- Use the minimum necessary confidential information.
- Access to confidential information should be on a strict need-to-know basis.
- Everyone with access to confidential information should be aware of their responsibilities.
- Comply with the law.
- The duty to share information for individual care is as important as the duty to protect patient confidentiality.
- Inform patients and service users about how their confidential information is used

18. All NHS organisations and local authorities that provide social services in England must have a Caldicott Guardian to uphold these principles and protect the

[7] https://ico.org.uk/

[8] Eight_Caldicott_Principles_08.12.20.pdf (publishing.service.gov.uk)

confidentiality of people's health and care information, making sure it is used properly[9].

19. All four nations have chosen to have Caldicott Guardians. These are represented by the UK Caldicott Guardian Council[10], which is a sub-group of the National Data Guardian's Panel[11] .

Policy

20. In England, the National Data Opt Out[12] also allows patients to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment, i.e. for research and planning.

21. There are some circumstances in which the Opt Out does not apply, for example:

- to anonymised, aggregate, or count type data
- where a patient has agreed to a specific use of data, e.g. to take part in a specific research project or clinical trial.
- where data is shared or disclosed for the purpose of monitoring and control of communicable disease or other risks to public health.
- where there is a legal requirement to disclose information.
- where the use or disclosure of information is in the overriding public interest.
- where there is a specific exemption, e.g. Public Health England National Disease Registers.

[9] Health Service Circular: HSC 1999/012 and Local Authority Circular: LAC 2002/2

[10] https://www.gov.uk/government/groups/uk-caldicott-guardian-council

[11] https://www.gov.uk/government/groups/independent-information-governance-oversight-panel

[12] https://digital.nhs.uk/services/national-data-opt-out