HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 07103, 28 April 2020

Patient health records: access, sharing and confidentiality

By
Elizabeth Parkin, Philip Loft

Inside:

1. Accessing and sharing patient health records
2. Sharing confidential patient information
3. Electronic health records
4. NHS data and cyber security
5. Patient Data, Apps and Artificial Intelligence (AI)
6. Cross-border data sharing after Brexit

Contents

Summary **3**

1. Accessing and sharing patient health records **4**
1.1 Charges to access records 5
1.2 Limiting access to health records 6
1.3 Parental access to child health records 6
1.4 Access to deceased patients' health records 7

2. Sharing confidential patient information **9**
2.1 Patient confidentiality and Covid-19 9
2.2 NHS Constitution and policy background 13
2.3 NHS Digital guidance on confidentiality 14
2.4 National Data Guardian for health and care Caldicott principles 14 15
2.5 National Data Guardian for health and care: priorities for 2019/20 16
2.6 National data opt-out programme 17
2.7 Legal and statutory disclosures of information 18
2.8 Disclosure of NHS data to the Home Office 19
2.9 Public interest disclosures of patient information 20
2.10 Deceased patients 21
2.11 Assessment of capacity to give or withhold consent 23
2.12 Private companies contracted to provide NHS services 24

3. Electronic health records **25**
3.1 NHS 'paper-free' by 2023 25
3.2 Summary Care Records 27

4. NHS data and cyber security **29**
4.1 National Data Guardian review (2016) 29
4.2 WannaCry Cyber Attack, 2017 30
4.3 Government response on cyber security 30

5. Patient Data, Apps and Artificial Intelligence (AI) **33**
5.1 Google DeepMind 34
5.2 Amazon Alexa 37
5.3 Telefonica 37
5.4 Coronavirus data store 38
5.5 Coronavirus-tracing app 38

6. Cross-border data sharing after Brexit **41**
6.1 Patient Data in Trade Agreements 41
6.2 US-UK Trade Agreement 41
6.3 Sharing Patient Data with the EU post-Brexit 42

Summary

Individuals have a right to access their own health records, and in limited circumstances, access to the records of other people. The Government has made a commitment that patients should gain access to their health records within 21 days following a request. Access to health records may also be granted in limited circumstances for relatives or in the case of deceased patients.

This briefing describes how patients may request access to their records, and the circumstances in which access to the records of others may be allowed, including new requirements introduced by the EU General Data Protection Regulation (GDPR) and the *Data Protection Act 2018*. It also describes statutory and public interest disclosures of patient information; information sharing rules for people who lack mental capacity; and access to information on hereditary conditions for relatives.

The Government has encouraged the NHS to make better use of technology, so that patients can manage their own healthcare needs, whilst ensuring that data remains safe at all times. It has also committed to all patients accessing their own care plan and communications from care professionals via the NHS app by 2020/21, and by 2023/24 patients will have access to digital-first primary care.

This briefing also outlines safeguarding arrangements for confidential patient information. In 2013, a review was carried out by the National Data Guardian for Health and Care, Dame Fiona Caldicott, to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve care.

In 2016, a subsequent review by Dame Fiona Caldicott looked at data security and patient opt-outs for the use of their data.

Recommendations from this review led to a number of changes in NHS data security policy, and the launch in May 2018 of a new national data opt-out program. In December 2018, the UK Parliament passed an Act placing the role of the National Data Guardian (NDG) for Health and Social Care on a statutory footing. This allows the NDG to issue statutory guidance about the processing of health and adult social care data.

The paper also details the recent treatment of patient data between the NHS and third-party groups such as Google and Amazon, and debates over the place of patient data in trade agreements after the UK's departure from the EU.

This briefing relates to the NHS in England, unless otherwise stated.

1. Accessing and sharing patient health records

Under current legislation, individuals have a right to access their own health records, and in limited circumstances, to access information about other people. This right extends equally to all relevant records relating to living individuals, including records held in the private health sector and health professionals' private practice records.

When an individual requests access to a health record, the request is processed by a 'data controller', which could be a GP or the organisation that a health professional is employed by, such as a hospital trust.[1]

Since 25 May 2018, access to patient health records is governed by the EU General Data Protection Regulation (GDPR), enacted by the *Data Protection Act 2018*. The new data protection legislation repealed the 1998 Data Protection Act. In 2010, the Department of Health produced *Guidance for Access to Health Records Requests*. This covered some other legislative basis for patients' access to their health records, including:

> **The Access to Health Records Act 1990** – which governs rights of access to deceased patient health records by specified persons.
>
> **The Medical Reports Act 1988** – which governs the right for individuals to have access to reports, relating to themselves, provided by medical practitioners for employment or insurance purposes[2]

No new Departmental guidance on access to health records has yet been published by NHS England intends to publish further information on GDPR and the NHS.

Under the 1998 DPA, an individual was required to request access to their health record in writing, although the earlier guidance did set out that requests could be made verbally where a patient was unable to submit a written request.[3] Under new data protection legislation there are no requirements for a patient to request their records in any specific way.[4]

The Information Governance Alliance (IGA) advises medical data controllers that regardless of whether the request is made verbally or in

---

1 NHS England, 'How do I get a copy of my health (medical) records?' (accessed 2 April 2020).
2 Department of Health, Guidance for Access to Health Records Requests (February 2010), p. 8.
3 Department of Health, Guidance for Access to Health Records Requests (February 2010), p. 9.
4 NHS England, 'How to access your personal information' (accessed 2 October 2019); Information Commissioner's Office, Preparing and submitting your subject access request (accessed 2 April 2020).

writing, they are required to check that the requestor is who they say they are.[5]

GDPR also reduces that amount of time within which requested medical records must be provided from 40 days to one month.[6] However, as set out in earlier guidance, the Government had made a commitment that health record requests should normally be handled within 21 days, despite the longer legal time limit under the 1998 DPA.[7]

Hospital records are generally kept for a minimum of eight years after treatment and GP records for a minimum of 10 years after a patient's death.[8] NHS organisations should retain records in accordance with the retention schedules outlined in Appendix Three of the 2016 IGA publication, Records Management Code of Practice for Health and Social Care.

1.1 Charges to access records

Previously, under the *Data Protection Act 1998* (DPA), data controllers of health records could charge between £10 and £50 for an access request, depending on where the records were held. However, since new data protection legislation came into force on 25 May 2018, record holders are no longer able to charge for accessing records.

The exception to this is where requests are 'manifestly unfounded or excessive'.[9] In these cases, the data controller can charge a reasonable fee to cover the administrative costs or refuse to act on the request. No specific amount is set out in legislation, but the *Data Protection Act 2018* allows for the Secretary of State to make regulations with regards to maximum fee levels.

However, the Government has said that insurance companies should continue to use the *Access to Medical Reports Act 1988* to obtain summary medical reports required for underwriting purposes from GPs.[10] The 1988 Act allows GPs to charge reasonable fees for such reports.[11]

A Parliamentary Question (PQ) answered in July 2018 explains the change:

> **Jackie Doyle Price:** The European Union General Data Protection Regulation (GDPR) came into effect from 25 May, replacing the Data Protection Act 1998. Within the updated regulation is the right of access, which gives individuals the right to obtain a copy of their personal data, including, from a health perspective, copies of medical records. Previously, under the Data Protection Act 1998, organisations were able to make a charge for dealing with

5 Information Governance Alliance, The EU General Data Protection Regulation: The Key Points for GPs (March 2018), p. 4.
6 Information Governance Alliance, The EU General Data Protection Regulation: The Key Points for GPs (March 2018), p. 4.
7 Department of Health, Guidance for Access to Health Records Requests (February 2010), p. 10
8 Records Management Code of Practice for Health and Social Care, Appendix 3.
9 *Data Protection Act 2018*, Chapter 2, Section 12.
10 Association of British Insurance, Access to Medical Records
11 *Access to Medical Reports Act 1988*, Section 4(4).

the administration required in such a request. Under the GDPR, the ability in law to levy such charges has been removed in most cases.

One exception to this principle is medical information required by insurance companies for underwriting purposes. The right of access under GDPR confers more personal information than is needed or is justified for insurance underwriting. Accordingly, insurance companies should instead use the established mechanism of the Access to Medical Reports Act 1988 (AMRA) to obtain summary medical reports from general practitioners (GPs). The AMRA allows the GP to charge a reasonable fee to cover the cost of copying the report.[12]

1.2 Limiting access to health records

There are certain circumstances in which full access to a patient's health records may be denied. These include cases where the release of health records is likely to cause serious harm to the physical or mental health of the subject or another individual. Therefore prior to release, the data controller should consult with either:

- The health professional responsible for the individual;
- Where there is more than one such health professional, the most suitable professional;
- Where no such professional is available, one with the experience and qualifications to advise accordingly.[13]

Where records do disclose information related to another individual, the data controller is not obliged to release the information, except in the following circumstances:

- The third party is a health professional who has compiled or contributed to the health records or who has been involved in the care of the patient;
- The third party, who is not a health professional, gives their consent to the disclosure of that information;
- It is reasonable to disclose without that third party's consent.[14]

1.3 Parental access to child health records

The British Medical Association (BMA) has produced guidance on confidentiality and the disclosure of health records. This explains that children who are aged 12 or over are generally expected to have capacity to give or withhold their consent to the release of information, and legally assumed to have the capacity when aged 16 or over in England, Wales and Northern Ireland. [15] In Scotland, anyone aged 12 and over is legally presumed to have such competence.[16]

---

12 PQ 162134, Medical Records, 12 July 2018

13 The *Data Protection (Subject Access Modification) (Health) Order 2000*, SI 2000/413. Similar provisions are included in Schedule 3 of the *Data Protection Act 2018*.

14 *Data Protection (Subject Access Modification) (Health) Order 2000*, SI 2000/413. Similar provisions are included in section 94(6) of the *Data Protection Act 2018*.

15 PQ, HL15330, Medical Records: Children, 24 April 2019

16 British Medical Association (BMA), Confidentiality and disclosure of health information tool kit (accessed 2 April 2020), pp. 27-8.

If a child has the capacity to give or withhold consent to the release of information from their health records, health professionals should respect their wishes. However, the guidance does state that every reasonable effort must be made to persuade the child to involve parents or guardians:

> **Competent children**
>
> […]
>
> If the child is competent to understand what is involved in the proposed treatment, the health professional should, unless there are convincing reasons to the contrary, for instance abuse is suspected, respect the child's wishes if they do not want parents or guardians to know. However, every reasonable effort must be made to persuade the child to involve parents or guardians particularly for important or life-changing decisions.
>
> **Children who lack capacity**
>
> The duty of confidentiality owed to a child who lacks capacity is the same as that owed to any other person. Occasionally, young people seek medical treatment, for example, contraception, but are judged to lack the capacity to give consent. An explicit request by a child that information should not be disclosed to parents or guardians, or indeed to any third party, must be respected save in the most exceptional circumstances, for example, where it puts the child at risk of significant harm, in which case disclosure may take place in the 'public interest' without consent. Therefore, even where the health professional considers a child to be too immature to consent to the treatment requested, confidentiality should still be respected concerning the consultation, unless there are very convincing reasons to the contrary. Where a health professional decides to disclose information to a third party against a child's wishes, the child should generally be told before the information is disclosed. The discussion with the child and the reasons for disclosure should also be documented in the child's record.[17]

There may also be instances where a relative may be provided access to patient information.

1.4 Access to deceased patients' health records

Access to deceased patients' health records is governed by the *Access to Health Records Act 1990*.

Under the terms of the Act, someone will only be entitled to access a deceased person's health records if they are either:

- a personal representative (the executor or administrator of the deceased person's estate);
- someone who has a claim resulting from the death (this could be a relative or another person)

[17] Ibid, pp. 34-5.

Access to a deceased person's health records may not be granted if a patient requested confidentiality whilst they were alive. No information can be revealed if the patient requested non-disclosure.[18]

Disclosure may also not take place if there is a risk of serious harm to an individual, or if records contain information relating to another person.[19]

For further information on patient confidentiality relating to deceased patients, see section 2.8 of this Briefing.

[18] *Access to Health Records Act 1990*, Chapter 23, 4(3)
[19] *Access to Health Records Act 1990*, Chapter 23, 5(1)(a)

2. Sharing confidential patient information

2.1 Patient confidentiality and Covid-19

Shielded Patients List

The NHS Covid-19: Shielded Patients List was developed to allow the NHS to identify and contact a group of patients who need specific advice about the Covid-19 outbreak. This list acted as the basis for official letters sent to around 900,000 individuals informing them that they should always stay at home for at least 12 weeks from the date they receive their letter. The Information Commissioner has said that:

> Data protection and electronic communication laws do not stop Government, the NHS or any other health professionals from sending public health messages to people, either by phone, text or email as these messages are not direct marketing. Nor does it stop them using the latest technology to facilitate safe and speedy consultations and diagnoses. […]
>
> The ICO [Information Commissioner's Office] is a reasonable and pragmatic regulator, one that does not operate in isolation from matters of serious public concern. Regarding compliance with data protection, we will take into account the compelling public interest in the current health emergency.[20]

The National Data Guardian, Dame Fiona Caldicott, has also backed this position.[21]

The list of shielded patients is disseminated by NHS Digital to organisations with which it has a data dissemination agreement in place. These agreements detail the terms of release and commitments for its use and handing. These organisations include the Cabinet Office, NHS Clinical Commissioning Groups, Capita (for distributing letters to shielded patients) and the NHS Business Service Authority (for sending text messages to shielded patients).[22]

Information is shared under Section 261(5)(c) of the *Health and Social Care Act 2012* ("the disclosure is necessary or expedient for the purposes of protecting the welfare of any individual"); Articles from the *General Data Protection Regulation 2016*: Article 6(1)(d) ("vital interests of the data subject or of another person") and Article 9(2(g) ("substantial public interest"); and Paragraph 6 of Schedule 1 to the *Data Protection Act 2018* ("these purposes are…[for] the exercise of a function of the Crown, a Minister of the Crown, or a Government Department).

The agreement with the Cabinet Office includes using a patient's name, date of birth, postcode and NHS number to verify the identity of the patient with whom they are seeking to contact. It also includes

---

20 Information Commissioner, Data protection and coronavirus, 12 March 2020
21 National Data Guardian, Data sharing during this public health emergency, 3 April 2020
22 NHS Digital, Distribution of the shielded patients list, 31 March 2020

agreements to share specific information with other Government Departments and outside bodies:

- Data will be cross-checked with the Department of Work and Pensions for the sole purposes of identifying deceased persons, missing phone numbers and establishing physical or financial vulnerability.
- The Department for the Environment of Food and Rural Affairs will receive necessary information to organise with supermarkets essential supplies to those patients who request support.
- The Ministry of Housing, Communities and Local Government will co-ordinate with local authorities if shielded patients have contacted them, known to receive social care, or known to be vulnerable. Local authorities are required to process confidential patient information under the guidance issued on 20 March 2020 (see below).[23]

Sharing Covid-19 Patient information

The Secretary of State for Health and Social Care, Matt Hancock, issued new guidance on 20 March 2020 under Regulation 3(4) of the *Health Service Control of Patient Information Regulations 2002*, allowing NHS England to process confidential information relating to patients if it is for a "Covid-19 Purpose and will be processed solely for that Covid-19 Purpose". This is in force until 30th September 2020 but can be extended.[24] The guidelines were distribution to GPs, local authorities, arm's length bodies of the DHSC, NHS Digital and Sir Simon Stevens, Chief Executive Officer of NHS England & Improvement.

A "Covid-19 Purpose" includes but is not limited to: understanding Covid-19; identifying and understanding information about patients or potential patients with, or at risk of, Covid-19; locating, contacting, screening and monitoring such patients; and delivering services to patients, clinicians, the health service and adult social care services workforce and the public in connection with Covid-19.[25]

Regulation 3 (1) of the 2002 Regulations allows confidential information to be processed for purposes including:

> (a) diagnosing communicable diseases and other risks to public health;
>
> (b) recognising trends in such diseases and risks;
>
> (c) controlling and preventing the spread of such diseases and risks;
>
> (d) monitoring and managing—
>
> (i) outbreaks of communicable disease;
>
> (ii) incidents of exposure to communicable disease;

---

23 NHS Digital, Letter to Cabinet Office with terms of release for the shielded patients list, 31 March 2020

24 Department of Health and Social Care (DHSC) to Organisations providing health services, General Practices, Local Authorities and Arm's Length Bodies of the DHSC, 20 March 2020, p. 1.

25 Ibid, pp. 2-3.

> (iii) the delivery, efficacy and safety of immunisation programmes;
>
> (iv) adverse reactions to vaccines and medicines;
>
> (v) risks of infection acquired from food or the environment (including water supplies);
>
> (vi) the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease.

Information may be shared to persons and organisations under regulation 3(3):

> (a) the Public Health Laboratory Service;
>
> (b) persons employed or engaged for the purposes of the health service;
>
> (c) other persons employed or engaged by a Government Department or other public authority in communicable disease surveillance.

NHS England & Improvement are only required to process confidential patient information if requested to do so by an authorised officer of the DHSC and the confidential information is required to be processed for a Covid-19 Purpose and will be solely processed for that purpose.

Data must also continue to be shared in line of Regulation 7 of the 2002 Regulations (for example, removing, as far as practical, anything that identifies a person and allowing only those owing a duty of confidentially and health professionals to process confidential patient information).[26]

Disclosure of deaths due to Coronavirus

During the Coronavirus outbreak, official statistics are being released stating the number of tests, cases and deaths related to Coronavirus.

The ONS Policy on disclosure control for births and deaths statistics is addressed to individuals and organisations that produce statistical outputs of birth, death or health data, such as Government Departments and NHS bodies. The policy pre-dates the Coronavirus outbreak. The policy is designed to "minimise the risk of unlawful disclosure of personal information". It states that:

> The mere fact of birth or death does not in itself reveal any protected information. For that reason, tabulations which reveal only that a certain number of births or deaths took place in a certain area and time period, even if it might be possible to identify an individual involved, do not usually need to be disclosure controlled.
>
> […] It is particularly important to be aware that, if a specific birth or death is revealed to be the only one of a particular age and sex combination or other readily identifiable characteristic in a known geographical area, there is a high risk of disclosure. It is therefore essential to check, for example, any sparse table containing cause of death by local authority (or smaller areas) against the

[26] DHSC to Simon Stevens, Covid-19 Notice, 20 March 2020, pp. 1-2.

> corresponding "all causes" figures for instances of obvious uniqueness.

During the Downing Street Press Conference on 29 March 2020, in response to a question on delays in the recording of deaths due to coronavirus, the Deputy Chief Medical Officer, Jenny Harries, said:

> We have to make sure when we're reporting [a death] the family is content and knows and that all our data is absolutely accurate…there is always a time lag for to check and evaluate the data across the system is linked [and] as we have had sadly to register more deaths that time period takes longer.[27]

There are three official statistical series on Coronavirus deaths:

- **DHSC figures** released on the Gov.UK website for the whole of the UK. This counts the number of deaths reported to the DHSC that have occurred in hospitals among patients who have tested positive for the Coronavirus (Covid-19) up until 5pm the day before. Data is added from the Devolved Administrations, though these have different cut off times. **This data is "only published once confirmed family have been notified of death"**.[28]
- **NHS England** deaths in hospital data includes patients who have tested positive for Coronavirus in England. It notes that "**confirmation of COVID-19 diagnosis, death notification and reporting in central figures can take up to several days** and the hospitals providing the data are under significant operational pressure. This means that the totals reported at 5pm on each day may not include all deaths that occurred on that day or on recent prior days."
- The **Office for National Statistics** provides figures based on all deaths registered involving Coronavirus according to death certification, whether in or out of hospital settings. This includes cases where Coronavirus is mentioned on the death certificate, even if no test for the virus occurred. Because the **ONS figures are derived from the formal process of death registration**, the ONS guide states "there is usually a delay of at least 5 days between occurrence and registration". It also says:

  > Numbers produced by the ONS take longer to prepare because they have to be certified by a doctor, registered and processed. But once ready, they are the most accurate and complete information.

  Parts 1-3 of Schedule 13 of the *Coronavirus Act 2020* contain temporary modifications to legislation relating to the registration of deaths across the UK. This allows registrations to occur by alternative methods (such as by telephone), for an alternative to the next of kin to register a death, and stated that Coronavirus, although a notifiable disease, "was not a reason of its own to notify the death to the coroner".[29]

---

27 No.10 YouTube Channel 29 March 2020 Press Conference, 12.53-13.25

28 Office for National Statistics, Deaths registered weekly in England and Wales, 7 April 2020, Table 2

29 UK Government, Revised guidance for registered medical practitioners of the Notification of Deaths Regulation, 2020, p.2

2.2 NHS Constitution and policy background

The NHS Constitution for England explains that patients have the right to privacy and confidentiality, the right to expect the NHS to keep patient confidential information safe and secure, and the right to be informed about how their information is used.[30]

Patients also have the right to request that their confidential information is not used beyond their own care and treatment, to have their objections considered, and, where their wishes cannot be followed, to be told the reasons including the legal basis.[31]

Policies on confidential patient data seek to strike a balance between the protection of patient information, and the use and sharing of information to improve care, such as for research purposes.

Patient information that is kept by health and social care providers must be securely safeguarded. Patient-doctor confidentiality is considered one of the cornerstones of medical practice. The BMA's Confidentiality and disclosure of health information tool kit states that:

> Confidentiality is an essential requirement for the preservation of trust between patients and health professionals and is subject to legal and ethical safeguards. Patients should be able to expect that information about their health which they give in confidence will be kept confidential unless there is a compelling reason why it should not.[32]

Individuals may also expect that relevant health information is shared among their care team to ensure high quality care, an integrated service and a better experience for patients. The *Health and Social Care (Safety and Quality) Act 2015* introduced a legal duty for health and social care professionals to share patient information where they consider that the disclosure is likely to facilitate patient care and is in the patient's best interest. The BMA opposed the introduction of this requirement, arguing in 2015 that:

> Health information sharing is governed by professional obligations to share relevant information for effective patient care, underpinned by patient consent. It is unnecessary to replace this with a statutory framework without clear justification as to why it is needed and which risks weakening confidentiality safeguards that currently apply.[33]

The sharing of anonymised patient information more widely can potentially bring about improvements to patient care. For example, tracking and analysis of patient health information can help with medical research and with the design of more effective services. NHS Digital is responsible for ensuring that information used in this way is

---

30 NHS England, NHS Constitution for England (July 2015) p. 8.
31 Ibid, p. 8.
32 BMA, Confidentiality and disclosure of health information tool kit (accessed 2 April 2020), p. 8.
33 BMA evidence to the Health and Social Care (Safety and Quality) Bill House of Lords Committee stage (13 March 2015), pp. 1-2.

suitably anonymised and untraceable to individuals before it is released..[34]

2.3 NHS Digital guidance on confidentiality

The *Health and Social Care Act 2012* gave NHS Digital (formerly the Health and Social Care Information Centre –HSCIC) a statutory duty to produce a Code of Practice for handling confidential information. This covers "the practice to be followed in relation to the collection, analysis, publication and other dissemination of confidential information concerning, or connected with the provision of health services or of adult social care in England."[35]

In September 2013, HSCIC published A guide to confidentiality in health and social care, which set out the confidentiality rules that should be followed in care settings run by the NHS or publicly funded adult social care services. The guide was based on the principles from the 2013 Caldicott Report and incorporated the good practice recommended by the Information Governance Review (see section 2.2).

The HSCIC guide set out five key principles for confidentiality:

- Confidential information about services users or patients should be treated confidentially and respectfully
- Members of a care team should share confidential information when it is needed for the safe and effective care of an individual
- Information that is shared for the benefit of the community should be anonymised
- An individual's right to object to the sharing of confidential information about them should be respected
- Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed[36]

The 1997 Caldicot Report recommended that senior individuals are appointed within NHS bodies to be responsible for following confidentiality procedures (these individuals are known as 'Caldicott Guardians').

2.4 National Data Guardian for health and care

In November 2014, Dame Fiona Caldicott was appointed as the first National Data Guardian (NDG) for health and care, to ensure patient trust in the use of their data and to review the balance between the protection and sharing of this data. The *Health and Social Care (National*

---

34 Wellcome Trust, 'Understanding patient data'; NHS England, 'How the NHS and care services use your information'

35 *Health and Social Care Act 2012*, 13S (1)

36 HSCIC, A guide to confidentiality in health and social care (September 2013), p.3. The guide is supported by a references document (September 2013) which provides more detailed information for organisations and examples of good practice.

Data Guardian) Act 2018 placed the role on a statutory footing.[37] The new law means that the NDG can issue official guidance about the processing of health and adult social care data to public bodies and private companies and charities which are delivering services for the NHS or publicly funded adult social care. In March 2019, Dame Caldicott was confirmed as NDG for a term of 18 months.

The NDG's terms of reference set out the three main principles that guided the pre-statutory role:

- encouraging clinicians and other members of care teams to share information to enable joined-up care, better diagnosis and treatment
- ensuring there are no surprises for the citizen about how their health and care data is being used and that they are given a choice about this
- building a dialogue with the public about how we all wish health and care information to be used, to include a range of voices including commercial companies providing drugs and services to the NHS, researchers discovering new connections that transform treatments, and those managing the services.[38]

Caldicott principles

In 2013, Dame Fiona Caldicott led a review into information governance of health data, Information: To Share Or Not To Share?

The 2013 Review set out seven revised principles to guide information governance – known as the 'Caldicott principles':

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

---

37 National Data Guardian (NDG), 'Dame Fiona Caldicott appointed as the first statutory National Data Guardian for Health and Social Care', 11 March 2019. The Library produced a briefing on the bill: Health and Social Care (National Data Guardian) Bill 2017-19 (2018).

38 NDG, Progress Report: January 2018-March 2019 (August 2019), Appendix C.

> Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
>
> **5. Everyone with access to personal confidential data should be aware of their responsibilities**
>
> Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.
>
> **6. Comply with the law**
>
> Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
>
> **7. The duty to share information can be as important as the duty to protect patient confidentiality**.
>
> Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The Caldicott Review also made 26 recommendations covering areas such as patients' access to electronic care records; information sharing among an individual's care team; opting-out of information sharing; and breaches of information governance.

The Government published its *Response to the Caldicott Review* in September 2013, and accepted in principle each of the 26 recommendations. The Government's response outlined how these recommendations will be implemented, and includes key commitments for health and social care providers, NHS England and organisations such as the Care Quality Commission (CQC).

2.5 National Data Guardian for health and care: priorities for 2019/20

In February 2019, the National Data Guardian for health and care launched a consultation on the proposed work priorities of the office. In response to the consultation, the NDG's new priorities were announced as:

> - Supporting public understanding and knowledge [of patient data and access to records]
> - Encouraging information sharing for individual care
> - Safeguarding a confidential health and care system.[39]

The NDG also conducted polling on public attitudes to organisations innovating with NHS data. The poll suggested that around half of people agreed that is fair for a partner university (49%) or partner

[39] NDG, Consultation response (July 2019), pp. 3-4.

private company (51%) to make a profit when developing technologies based on the use of NHS data. 73% believed that the NHS should benefit, by accessing new technologies or medicines at a reduced cost. The NDG used these results to argue that "supporting and extending this public conversation [on how benefits from patient data can be shared to the benefit of the NHS] is crucial if we are to gain from the rich information held safely in the health and care system and retain public trust."[40]

2.6 National data opt-out programme

On 25 May 2018, NHS Digital launched the national data opt-out programme, a tool that allows patients to choose to opt out of their data being shared outside of the NHS. This is an online system, but a non-digital alternative is provided for patients who cannot or do not want to use an online system. Unlike its predecessor, Care.data, there is a single opt-out point applied across the system, and a mechanism for people to register their choice.[41]

The national programme will replace the existing system of Type 1 and Type 2 opt-outs (as well as a number of local opt-out systems).[42] Type 2 opt-outs, where patients register with their GP to prevent their information being shared with organisations outside the NHS, will be automatically converted to the national data opt-out programme, and patients will be informed individually.[43]

Type 1 opt-outs, where patients register with their GP practice to prevent their identifiable data leaving the practice for purposes beyond their individual care, will continue to be respected until 2020 when the Department of Health and Social Care (DHSC) will consult with the NDG on their removal.[44]

Although the opt-out tool was launched on 25 May 2018, health and care organisations were not expected to comply until March 2020. Due to the Covid-19 outbreak, the compliance deadline has been extended to 30 September 2020, at which point the position will be reviewed. NHS Digital have said that "organisations that are already compliant should continue as appropriate".[45]

The programme was originally planned to have been launched in March 2018,[46] but was delayed to coincide with new data protection legislation coming into force.

---

40 NDG, 'NDG poll findings: public attitudes to organisations', 2 July 2019.
41 Understanding Patient Data, 'Is the new national data opt-out just Care.data all over again?', 25 May 2018.
42 NHS Digital, 'Opting out of sharing your confidential patient information', 7 March 2019.
43 NHS Digital, 'Collection and conversion of type 2 opt-outs', 7 March 2019.
44 NHS Digital, 'Information for GP practices', 3 September 2019.
45 NHS Digital, 'National data opt-out' ; NHS Digital and NHSX to NHS England, 19 March 2020
46 Department of Health, 'Your data: Better security, better choice, better care' (July 2017), p. 23.

As of March 2019, 2.7% of registered patients had an active national data opt-out of either Type 1 or 2, or 1.64 million patients.[47] This compared to 1.6 million in July 2018.[48]

The new system is based on a recommendation by the NDG, Dame Fiona Caldicott, in the 2016 Review of Data Security, Consent and Opt-Outs. The review was launched following the suspension of the national Care.data programme, due to concerns over the opt-out system in place and over patient confidentiality.[49] Following the review, the then Life Sciences Minister George Freeman confirmed in July 2016 that Care.data was to be closed.[50]

The Government's response to the NDG review confirmed that the national data opt-out programme would not apply to information anonymised in line with the Information Commissioner's Office Code of Practice on Anonymisation.

2.7 Legal and statutory disclosures of information

There are certain circumstances in which a health professional is required by law to disclose medical information, regardless of patients consent. For example, statutory disclosures are required under the following legislation, although this is not an exhaustive list:

- *Health Protection (Notification) Regulations 2010* – a health professional must notify local authorities about any person suspected of having a range of listed conditions, including food poisoning, measles and tetanus.
- *Abortion Regulations 1991* – a doctor carrying out a termination of pregnancy must notify the Chief Medical Officer, giving the individual's date of birth and postcode.
- *Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013* – deaths, major injuries and accidents resulting in three days off work, as well as certain diseases and dangerous occurrences, must be reported.
- *Female Genital Mutilation Act 2003* – medical professionals must inform the chief police officer for the area where they learn of or suspect female genital mutilation of a girl aged under 18.

The BMA provides additional information on legal and statutory disclosures. Some statutes allow, rather than mandate, disclosure of confidential information. For example, under the *Children Act 1989*, disclosure is permitted to other organisations such as the police or social services if there is a suspicion that a child is suffering, or is at risk of suffering, significant harm.[51] Under section 261 of the *Health and Social*

47 NHS Digital, 'National Data Opt-Out, March 2019'
48 NHS Digital, 'National Data Opt-Out, July 2018'
49 Care.data was a system to extract and link large amounts of patient data collected as part of NHS care. Further background information on Care.data can be found in the archived Commons Library briefing paper SN06781 (2014).
50 Care Quality and National Data Guardian for Health and Care's Independent Reviews into Data Security, HCWS626 July 2016
51 BMA, Confidentiality and disclosure of health information tool kit (accessed 2 April 2020), pp. 34-5.

Care Act 2012, NHS Digital is permitted to disclose information in certain circumstances, including in connection with the investigation of a criminal offence.

In contrast, some statutes require health professionals to restrict disclosure of certain confidential information. For example, under the *Gender Recognition Act 2004*, it is an offence to disclose protected information such as a person's gender history after that person has changed gender.

Patient confidentiality can also be overridden under section 251 of the *NHS Act 2006*, which allows for the Secretary of State to set aside the duty of confidentiality for the purposes of research, audit and other medical purposes that are not directly related to a patient's care.[52]

2.8 Disclosure of NHS data to the Home Office

Section 261 of the *Health and Social Care Act 2012* is the legal basis of a Memorandum of Understanding (MoU) between the Home Office, NHS Digital and the Department of Health, published in 2017, and withdrawn in 2018. This allowed NHS Digital to pass information about patients to the Home Office, where the individual was suspected of an immigration offence.

Concerns were raised by organisations, including Public Health England, that the passing of confidential information to the Home Office could deter individuals from seeking healthcare, which could in turn impact on public health.[53] In light of these concerns, in January 2018, the Chair of the Health Select Committee, Dr Sarah Wollaston MP, wrote to NHS Digital requesting that they withdraw from the MoU.[54] A subsequent letter to the Committee from the Government noted these concerns, but argued that there was no cause for a significant change of approach.[55]

During the Report Stage debate of the *Data Protection Bill 2017-19*, Dr Wollaston proposed an amendment to the Bill, which would have meant that NHS Digital could only share data when requested by a police force for the investigation of a serious offence.[56]

In response, the Digital and Creative Industries Minister, Margot James, announced a change in approach in May 2018:

---

52 HSCIC, A guide to confidentiality in health and social care (September 2013), p. 21.
53 Health Committee, Correspondence regarding memorandum of understanding between NHS Digital, Home Office and the Department for Health on data sharing (2017), 'PHE Response: Feb 2017', p. 1.
54 Health Committee, Letter to Sarah Wilkinson, Chief Executive, NHS Digital, regarding sharing of patient address information with the Home Office for immigration enforcement purposes, 29 January 2018.
55 Caroline Nokes MP, Minister of State for Immigration, Home Office, and Lord O'Shaughnessy, DHSC, Letter regarding letter from the Chair to NHS Digital on the Memorandum of Understanding with the Home Office, 23 February 2018.
56 HC Deb Data Protection Bill (Lords), vol. 640, c 770, 9 May 2018

> The Government have reflected further on the concerns put forward by my hon. friend (Dr Wollaston) and her Committee. As a result, and with immediate effect, the data sharing arrangements between the Home Office and the NHS have been amended. This is a new step and it supersedes the position set out in previous correspondence between the Home Office, the Department for Health and Social Care and the Select Committee.
>
> […]
>
> My right hon. Friend the Minister for Immigration is committed to sending a copy of an updated shortly, but as I have indicated, the significant narrowing of the MOU will have immediate effect. This commitment is consistent with the intention underpinning new clause 12.[57]

The amendment was withdrawn. On 28 January 2019, the DHSC, the Home Office and NHS Digital stated that "they will continue to work together to agree how future information requests will be processed."[58] Public Health England conducted a review on the potential impact of a new MoU on public health, ending in April 2019.[59] Public Health England are currently analysing feedback (April 2020).[60]

An amendment was proposed by Kate Green MP to the Coronavirus Bill 2020 to "cease all data sharing between the Home Office and NHS Digital, any NHS trust or any other part of the National Health Service" in connection with NHS charging, the "compliant environment", or any other immigration funding. The amendment was not passed.[61]

Data sharing between the NHS and the Home Office on the reporting of patient's subject to immigration rules with a total NHS debt of over £500 to the Home Office, was unaffected by the MoU's withdrawal.[62]

2.9 Public interest disclosures of patient information

There are also exceptional circumstances in which a health or social care professional may be obliged to share confidential patient information in line with the "public interest." The BMA describes this type of mandatory disclosure:

> Disclosures in the public interest based on the common law are made where disclosure is essential to prevent a serious and imminent threat to public health, national security, the life of the individual or a third party or to prevent or detect serious crime.[63]

---

57 HC Deb Data Protection Bill (Lords), vol. 640, cc 756-8, 9 May 2018
58 DHSC, 'Information requests from the Home Office to NHS Digital', 28 January 2019.
59 PQ 211731, Health Services: Immigrants, 23 January 2019
60 Public Health England, 'Data sharing MoU between NHS Digital and Home Office' (accessed 2 April 2020).
61 Coronavirus Bill: Committee of the Whole House, 23 March 2020
62 DHSC, Overseas chargeable patients, NHS debt and immigration rules (26 March 2019).
63 BMA, Confidentiality and disclosure of health information tool kit (accessed 2 April 2020), p. 44.

Informed consent from the individual must always be sought first, but an individual's right to confidentiality can be overruled to protect the public interest.[64]

NHS Digital also provides guidance on sharing genetic information with family members, where the diagnosis of a condition in the patient might point to the likelihood of the same condition in a blood relative. In circumstances where a patient refuses to give consent to share information, disclosure might still be justified in the public interest. It recommends that:

> If a patient refuses consent to disclosure, health and care staff will need to balance their duty to make the care of the patient their first concern against their duty to help protect the other person from serious harm. If practicable, health and care staff should not disclose the patient's identity in contacting and advising others of the risks they face.[65]

2.10 Deceased patients

There is still an ethical obligation to respect a patient's confidentiality for deceased patients. The Information Tribunal in England and Wales has held that a duty of confidentiality applies to the health records of deceased patients under section 41 of the *Freedom of Information Act 2000*.[66] The Department of Health and Social Care, General Medical Council (GMC) and other clinical professional bodies have also long accepted that the duty of confidentiality continues beyond death and this is reflected in the guidance they produce.[67]

Under the terms of the *Access to Health Records Act 1990*, someone will only be able to access a deceased person's health records if they are either:

- a personal representative (i.e. the executor or administrator of the deceased person's estate); or
- or someone who has a claim resulting from the death (this could be a relative or another person).[68]

Access to a deceased person's health records may not be granted if a patient requested confidentiality whilst they were alive. No information can be revealed if the patient requested non-disclosure. Disclosure may also be prevented if there is a risk of serious harm to an individual, or if the records contain information relating to another person.[69]

The GMC sets out the circumstances in which information from a deceased's person's health records should be disclosed:

> Your duty of confidentiality continues after a patient has died.

---

64 HSCIC, A guide to confidentiality in health and social care (September 2013), p. 20.
65 HSCIC, A guide to confidentiality in health and social care: references (September 2013), p. 25.
66 BMA, Confidentiality and disclosure of health information toolkit (accessed 2 April 2020), p. 49.
67 Department of Health, Guidance for Access to Health Records Requests (February 2010), p. 13.
68 *Access to Health Records Act 1990*, Chapter 23, 4(3)
69 *Access to Health Records Act 1990*, Chapter 23, 5(1)(a)

There are circumstances in which you must disclose relevant information about a patient who has died. For example:

- when disclosure is required by law
- to help a coroner, procurator fiscal or other similar officer with an inquest or fatal accident inquiry
- on death certificates, which you must complete honestly and fully
- when a person has a right of access to records under the *Access to Health Records Act 1990* or the *Access to Health Records (Northern Ireland) Order 1993*, unless an exemption applies
- when disclosure is necessary to meet a statutory duty of candour.

In other circumstances, whether and what personal information may be disclosed after a patient's death will depend on the facts of the case. If the patient had asked for information to remain confidential, you should usually abide by their wishes. If you are unaware of any instructions from the patient, when you are considering requests for information you should take into account:

- whether disclosing information is likely to cause distress to, or be of benefit to, the patient's partner or family
- whether the disclosure will also disclose information about the patient's family or anyone else
- whether the information is already public knowledge or can be anonymised or de-identified
- the purpose of the disclosure.

Circumstances in which you should usually disclose relevant information about a patient who has died include:

- the disclosure is permitted or has been approved under a statutory process that sets aside the common law duty of confidentiality, unless you know the patient has objected
- when disclosure is justified in the public interest to protect others from a risk of death or serious harm
- for public health surveillance, in which case the information should be anonymised, unless that would defeat the purpose
- when a parent asks for information about the circumstances and causes of a child's death
- when someone close to an adult patient asks for information about the circumstances of that patient's death, and you have no reason to believe the patient would have objected to such a disclosure
- when disclosure is necessary to meet a professional duty of candour
- when it is necessary to support the reporting or investigation of adverse incidents, or complaints, for local clinical audit, or for clinical outcome review programmes.

Archived records relating to deceased patients remain subject to a duty of confidentiality, although the potential for disclosing

> information about, or causing distress to, surviving relatives or damaging the public's trust will diminish over time.[70]

2.11 Assessment of capacity to give or withhold consent

If a patient lacks the mental capacity to either give or withhold their consent to disclosure of confidential information, medical information may need to be shared with relatives, friends and carers to enable health professionals to determine their best interests. The BMA advises that:

> Where a patient is seriously ill and lacks capacity, it would be unreasonable always to refuse to provide any information to those close to the patient on the basis that the patient has not given explicit consent. This does not, however, mean that all information should be routinely shared, and where the information is sensitive, a judgement will be needed about how much information the patient is likely to want to be shared, and with whom. Where there is evidence that the patient did not want information shared, this must be respected.[71]

Patients who may have a mental health condition do not automatically lack this capacity. However, under the *Mental Health Act 1983*, qualifying patients are entitled to support from an Independent Mental Health Advocate (IMHA). Subject to certain criteria, section 130B of that Act provides that, in order to provide help to a qualifying patient, IMHAs may require the production of and inspect any records relating to the patient's detention or treatment in any hospital or to any after-care services provided for the patient under section 117 of the Act.[72]

The Modernising the Mental Health Review, which reported in December 2018, recommended that:

> 13. Patients should be able to choose a new Nominated Person (NP) to replace the current Nearest Relative (NR) role under section 26 of the MHA [Mental Health Act].
>
> (,,,)
>
> 15. Patients should have greater rights to choose to disclose confidential information to additional trusted friends and relatives, including through the NP nomination process or advance choice documents.[73]

The Government has committed to publish a white paper on reform to the Mental Health Act "as soon as it possible to do so" and consult on legislation and bring forward a bill "when parliamentary time allows".[74]

---

70 General Medical Council, Ethical Guidance for Doctors: 'Managing and Protecting Personal Information' (last accessed 4 April 2020).

71 BMA, Confidentiality and disclosure of health information tool kit (accessed 2 April 2020), pp.30-1.

72 Department of Health, Code of Practice: Mental Health Act 1983, Chapter 20.

73 Modernising the Mental Health Act: Increasing choice, reducing compulsion (December 2018), p. 89.

74 PQ 30679, Mental Health Act 1983 Independent Review, 17 March 2020

2.12 Private companies contracted to provide NHS services

All providers of NHS care, whether NHS or NHS bodies, are governed by the *Health and Social (Safety and Quality) Act 2015*, inserted section 251B of the Health and Social Care Act 2012. This provides a duty on information to be shared where it facilitates care for an individual and it is legal to do so. This sharing requires the patient to be informed and provide them with an opportunity to object. The Act followed the Caldicott Review in 2013.

The answer to the below PQ sets out that private sector providers contracted to provide direct care to NHS patients are expected to share and receive patient information for treatment and care of an individual:

> **Julian Knight:** To ask the Secretary of State for Health, what obligations private hospitals and NHS foundation trusts have to share the medical records of patients who have used both services (a) in general and (b) when such trusts have referred patients to private hospitals.
>
> **George Freeman:** We expect that all of the organisations involved in providing direct care to a National Health Service patient, irrespective of whether they are an NHS provider or a private sector provider under contract to the NHS, will share information that is relevant to the safe and timely provision of treatment and care.
>
> The only exception should be if the patient objects to information about them being shared. This approach is consistent with the Caldicott Principles which state that "the duty to share data can be as important as the duty to protect confidentiality." The duty to share information as described in Section 251B of the Health and Social Care Act 2012.[75]

An answer to a PQ of October 2018 describes how private providers must provide data with the NHS for secondary uses (such as health care planning or commissioning of services):

> **Stephen Barclay:** Private companies that are awarded contracts to provide NHS services are bound by the same obligations as public providers of NHS care regarding the provision of data for secondary uses. Where a national data collection is established, all contracted providers, whether privately or publicly owned, are required to respond in accordance with the collection guidance issued for that individual collection. The NHS Standard Contract Service terms and conditions require all contracted providers to meet obligations to provide data.[76]

---

75 PQ, 37056, Medical Records: Disclosure of information, 24 May 2016
76 PQ, 179140, Medical Records 15 October 2018

3. Electronic health records

3.1 NHS 'paper-free' by 2023

Original Timescale

In a speech on 2 September 2015, the Health Secretary, Jeremy Hunt, outlined the Government's vision for the use of technology across the NHS. The accompanying press release set out a timetable for reform:

> Mr Hunt made clear that by 2016 all patients should be able to access their own GP electronic record online in full, seeing not just a summary of their allergies and medication but blood test results, appointment records and medical histories. By 2018 this record will include information from all their health and care interactions.
>
> […]
>
> In addition, by the end of 2018 all doctors and nurses will be able to access the most up-to-date lifesaving information across GP surgeries, ambulance services and A&E departments, no matter where a patient is in England. By 2020 this will include the social care system as well.[77]

NHS England's Five Year Forward View (5YFV; October 2014), committed to making all patients' records "largely paperless" by 2020. The 5YFV committed the new National Information Board to publishing plans to develop fully interoperable electronic health records so that patients' records are largely paperless. Patients will have full access to these records, and be able to write into them. They will retain the right to opt out of their record being shared electronically. The NHS number, for safety and efficiency reasons, will be used as an identifier in all settings, including social care.[78]

In November 2014, the National Information Board published Personal Health and Care 2020: Using Data and Technology to Transform Outcomes for Patients and Citizens: A Framework for Action. The framework set out the Government's policy for using information technology to improve the delivery of healthcare and transform outcomes for patients and citizens, as well as how better use of digital technology could benefit patients, reduce care costs and improve patient safety. With regards to electronic health records, the framework stated that:

> In 2015, all citizens will have online access to their GP records and will be able to view copies of that data through apps and digital platforms of their choice. But it is essential that citizens have access to all their data in health and care, and the ability to 'write' into it so that their own preferences and data from other relevant sources, like wearable devices, can be included. Patients won't have the ability to edit the entries their clinician has made but their comments will be visible. This framework prioritises

---

77 Department of Health and National Information Board, 'Health Secretary outlines vision for use of technology across NHS', 2 September 2015.

78 NHS England, Five Year Forward View, October 2014.

> comprehensive access – with the ability for individuals to add to their own records – by 2018.[79]
>
> […]
>
> All patient and care records will be digital, real-time and interoperable by 2020. By 2018 clinicians in primary, urgent and emergency care and other key transitions of care contexts will be operating without needing to use paper records. This will be achieved by alignment of national technical and professional data standards with regulatory and commissioning requirements. By April 2015, building on the existing interoperability programme, the NIB, in partnership with users and industry bodies, including the Foundation Trust Network and the NHS Confederation, will coordinate agreement on these standards and how they should be 'hard-wired' into commissioning and regulatory oversight.[80]

The framework also stated that in April 2016 the Health and Social Care Information Centre (now NHS Digital) would consult on ways of supporting carers to access digital records.[81]

As of January 2017, all local health and care systems have produced Local Digital Roadmaps, setting out how they will achieve the ambition of 'paper-free at the point of care' by 2020.[82]

Further background information on electronic health records can be found in the Parliamentary Office of Science and Technology (POST) briefing on electronic health records (2016), which looks at the current use and potential benefits of electronic health records, and challenges to implementation, including IT systems and data security and privacy

Revised Timescale

A Government commissioned review of NHS IT by Robert Wachter reported in September 2016. It stated that the "target of 'paperless by 2020' should be discarded as unrealistic." It set 2023 as a reasonable goal to have all trusts largely digitised, if the Treasury provided funds additional to the £4.2 billion announced in 2016.[83] The then-Health Secretary, Jeremy Hunt, supported the revised timetable for digitising the NHS.[84] The October 2018 Future of Healthcare Policy Paper re-iterated the Government's desire to provide greater digital infrastructure for the NHS. The NHS Long Term Plan, published in January 2019, stated that all providers, across acute, community and mental health settings, will be expected to advance to a core level of digitisation by 2024:

> • During 2019 we will introduce controls to ensure new systems purchased by the NHS comply with agreed standards, including those set out in The Future of Healthcare.

---

79 National Information Board, Personal Health and Care 2020 (November 2014), p. 21.
80 Ibid, p. 29.
81 Ibid, p. 31.
82 NHS England, Local Digital Roadmaps
83 Making IT Work: Harnessing the power of health information technology to improve care in England (7 September 2016)
84 National Health Executive, 'NHS IT, records and data', 8 September 2016.

- By 2020, five geographies will deliver a longitudinal health and care record platform linking NHS and local authority organisations, three additional areas will follow in 2021.
- In 2020/21, people will have access to their care plan and communications from their care professionals via the NHS App; the care plan will move to the individual's LHCR across the country over the next five years.
- By summer 2021, we will have 100% compliance with mandated cyber security standards across all NHS organisations in the health and care system.
- In 2021/22, we will have systems that support population health management in every Integrated Care System across England, with a Chief Clinical Information Officer (CCIO) or Chief Information Officer (CIO) on the board of every local NHS organisation.
- By 2022/23, the Child Protection Information system will be extended to cover all health care settings, including general practices.
- By 2023/24 every patient in England will be able to access a digital first primary care offer.
- By 2024, secondary care providers in England, including acute, community and mental health care settings, will be fully digitised, including clinical and operational processes across all settings, locations and departments. Data will be captured, stored and transmitted electronically, supported by robust IT infrastructure and cyber security, and LHCRs will cover the whole country. [85]

3.2 Summary Care Records

The NHS in England is also rolling out Summary Care Records (SCRs), which are electronic health records containing essential information about a patient, such as their medication, allergies and adverse reactions. A reasonable adjustment 'digital flag' will also be added to the summary care record by 2023/24 in order to alert NHS staff of patients with a learning disability or autism.[86] Patients can also choose to include additional information, such as long-term conditions and specific communication needs.

The NHS Digital page on SCRs sets out their key functions:

- Professionals across care settings can access GP held information on GP prescribed medications, patient allergies and adverse reactions (SCR core functionality)
- Clinicians in urgent and emergency care settings can access key GP-held information for patients previously identified by GPs as most likely to present in urgent and emergency care) (SCR with additional information)
- Professionals across care settings made aware of end-of-life preference information (SCR with additional information)[87]

Health and care professionals must have a smart card with the correct codes to access an SCR. All usages must be logged, and a patient can

85 NHS England, NHS Long Term Plan (January 2019), pp. 96, 99.
86 PQ, 259275, Autism and Learning Disability, 11 June 2019
87 NHS Digital, Summary Care Records (SCR) (last accessed 2 April 2020).

make a subject access request to see who has looked at their SCR. In addition, professionals must seek a patient's permission if they need to look at the SCR. If they can't ask because the patient is unconscious or otherwise unable to communicate, they may decide to look at the SCR because doing so is deemed to be in the patient's best interest. Patients can also opt out of having a SCR by contacting their GP.[88]

As of December 2017, 98% of the population in England have a Summary Care Record. In 2017, SCRs were expected to be used around 6.5 million times, up from 4 million in 2016.[89]

In February 2019, the European Commission recommended the creation of a European Electronic Health Record, with the aim of producing a common format of health information that would enable patient information to be shared more easily across the EU.[90]

SCRs in Community Pharmacies

Rollout of SCRs also covers community pharmacies. As of July 2018, 95% of pharmacies in England had access to the Electronic Prescription Service and Summary Care Record.[91] In October 2017, 80% of Pharmacies had a secure NHS email account to contact GPs regarding patient encounters.[92] A survey of English Pharmacies by the *Pharmaceutical Journal* in the summer of 2018 found that only 34% of the 1,200 pharmacies surveyed accessed the SCR at least once a week.[93]

88 NHS Digital, 'Viewing Summary Care Records (SCR)' (last accessed 2 April 2020); Summary Care Records (SCR) (last accessed 2 April 2020).
89 PQ, 115038, NHS: Digital Technology, 1 December 2017
90 European Commission, 'Recommendation on an European Electronic Health Record Exchange Format', 6 February 2019.
91 PQ, 165012, Pharmacy: Digital Technology, 23 July 2018
92 PQ, 107291, Pharmacy: Medical Records, 19 October 2017
93 Emma Wilkinson, 'Why are so few pharmacies using the summary care record?', *The Pharmaceutical Journal*, 25 October 2018.

4. NHS data and cyber security

4.1 National Data Guardian review (2016)

A major review of NHS data security was carried out by the National Data Guardian for health and care, Dame Fiona Caldicott, in 2016. The Review of Data Security, Consent and Opt-Outs set out a number of recommendations to improve security, including requirements for leaders of NHS organisations to demonstrate responsibility for data security, harsher sanctions from the Government for data security breaches, and allowing the Care Quality Commission (CQC) to inspect NHS providers against their data security standards.

The review also set out 10 data security standards that the NHS should adhere to:

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.
4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.
9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and

> meeting the National Data Guardian's Data Security Standard.[94]

4.2 WannaCry Cyber Attack, 2017

On 12 May 2017, a global ransomware cyberattack, known as WannaCry, attacked a range of companies and sectors, including the NHS. A later NAO investigation found that the 2017 ransomware attack impacted on 80 of the 236 NHS Trusts in England, plus a further 603 primary care and other organisations, and led to an estimated 19,000 patient appointments being cancelled.[95] It is estimated that the WannaCry cyber-attack cost the NHS £92 million. This figure does not include other organisations also impacted on by the cyber-attack.[96] The NHS investigation found that none of the 80 NHS Trusts affected by WannaCry had applied an advised Microsoft patch update.[97]

In response to the 2017 WannaCry ransomware attack on the NHS, the Public Accounts Committee highlighted the ongoing threat that cyberattacks could pose to the security of patient data:

> WannaCry was a financially motivated ransomware attack, and as such relatively unsophisticated (it locked devices but did not seek to alter or steal data). However, future attacks could be more sophisticated and malicious in intent, resulting in the theft or compromise of patient data. The Department and its arm's-length bodies accept that cyber-attacks are now a fact of life and that the NHS will never be completely safe from them.[98]

4.3 Government response on cyber security

In its July 2017 response to the review, the Government accepted the recommendations of the Caldicott Review and confirmed that a new Information Governance Toolkit was being developed to implement the data security standards. This was launched in April 2018, as the Data Security and Protection Toolkit.

The response expanded on data standard number 6, noting that serious cyber-attacks should be reported to CareCERT[99] immediately.[100] It also confirmed that harsher sanctions for malicious or intentional data security breaches would be brought in by the new 2018 data protection legislation.[101]

In addition to these requirements, as of 25 May 2018, under the *Data Protection Act 2018* and GDPR, NHS organisations are required to

---

94 NDG, *Review of Data Security, Consent and Opt-Outs*, June 2016
95 National Audit Office, Investigation: WannaCry cyber-attack and the NHS (25 April 2018), p.4.
96 DHSC, Securing cyber resilience in health and care: progress update October 2018 (October 2018), p. 14.
97 NHS Improvement, Lessons learned review of the WannaCry Ransomware Cyber Attack (February 2018), p. 8.
98 Committee of Public Accounts, Cyber-attack on the NHS (28 March 2018), HC 787 2017-19, para 19.
99 NHS Digital's Care Computer Emergency Response Team
100 Department of Health, Your data: Better security, better choice, better care (July 2017), p. 53.
101 Ibid, p. 46.

inform the Information Commissioner's Office within 72 hours of any personal data breach. Patients whose data has been breached must also be contacted and informed under the new data protection requirements.[102]

In answer to a Parliamentary Question of September 2018 requesting an update on the Government response to the cyber-attack of May 2017, the Government stated:

> **Jackie Doyle Price:** The National Health Service is putting in place robust measures to protect IT systems against cyber-attacks. Since May 2017 the Government has invested £60 million to support NHS providers to improve their security position, with a further £150 million pledged up until 2021 to improve the NHS's resilience against attacks.
>
> The Department published its progress report in February 2018 entitled 'Securing cyber resilience in health and care: progress update'. The report is available at the following link:
>
> https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-progress-update
>
> Key actions taken since February 2018 include:
>
> - signing a Windows 10 licensing agreement with Microsoft which will allow local NHS organisations to save money, reduce potential vulnerabilities and help increase cyber resilience;
>
> - enhancing the capability of the Cyber Security Operations Centre boosting the national capability to prevent, detect and respond to cyber-attacks through the procurement of IBM as a specialist partner;
>
> - launching the Data Security and Protection Toolkit which provides an accessible dashboard enabling trusts to track their progress in meeting the 10 Data Security Standards;
>
> - agreeing plans to implement the recommendations of the Chief Information Officer for Health and Care's review of the May 2017 WannaCry attack;
>
> - provided specialist face to face security training (System Security Certified Practitioner - SSCP) for over 100 staff; and
>
> - in May 2018 the Network and Information Security Regulations came into force which requires operators of essential services (including some NHS healthcare providers) to put appropriate security measures in place and to report significant incidents that occur.[103]

The Department made a fuller announcement of new NHS cyber security improvements in April 2018. In addition to the above, these included:

> A new digital security operations centre to prevent, detect and respond to incidents.
>
> The centre will:
>
> - allow NHS Digital to respond to cyber attacks more quickly

[102] Information Commissioner's Office, 'Personal data breaches' (accessed 2 April 2020).

[103] PQ, 169018, NHS: Cybercrime, 3 September 2018

- allow local trusts to detect threats, isolate infected machines and kill the threat before it spreads

Other measures to improve cyber security include:

- £21 million to upgrade firewalls and network infrastructure at major trauma centre hospitals and ambulance trusts
- £39 million spent by NHS trusts to address infrastructure weaknesses
- new powers given to the Care Quality Commission to inspect NHS trusts on their cyber and data security capabilities

  […]

- a text messaging alert system to ensure trusts have access to accurate information – even when internet and email services are down[104]

Freedom of Information Requests to 226 NHS Trusts found that 43 had not allocated any funding for cybersecurity between August 2017 and August 2018. 67 Trusts did not respond.[105]

Government progress on NHS cyber resilience was further set out in a report of October 2018.[106] One recommendation from the NHS CIO's WannaCry report (4.7) was for NHS organisations to move to compliance with the "Cyber Essentials Plus" standard by June 2021. As of September 2019, 70% of "large NHS organisations" have met this standard, compared to 19% in February 2018.[107]

In 2019, the Department stated that it was continuing to support NHS organisations to upgrade their existing Windows systems to reduce potential vulnerabilities,[108] and that £250 million will have been invested nationally to improve the cyber security of the health and social care system between 2016 and 2021.[109] At the time of the cyber-attack in 2017, 5% of the NHS estate was using old software such as Windows XP, despite having been advised to upgrade by the Department of Health since 2014.[110] In July 2019, 0.16% of NHS Machines were still using Windows XP.[111]

---

104 DHSC, 'Plans to strengthen NHS cyber security announced', 28 April 2018
105 'One in four NHS trusts spent no money on cybersecurity last year', Financial Times, 11 December 2018.
106 DHSC, 'Securing cyber resilience in health and care', October 2018
107 NHS Digital, 'How we're improving cyber security', 8 October 2019.
108 PQ, 252873, NHS: Cybercrime, 20 May 2019
109 PQ, 254786, NHS Cybercrime, 15 May 2019
110 Committee of Public Accounts, Cyber-attack on the NHS, 28 March 2018, HC 787 2017-19, paras 5-7.
111 PQ 277855, NHS: Computer Software,16 July 2019

5. Patient Data, Apps and Artificial Intelligence (AI)

In October 2018, the Secretary of State for Health and Social Care, Matt Hancock, stated on the launch of The Future of Healthcare, "robust standards will ensure that every part of the NHS can use the best technology to improve patient safety, reduce delays, and speed up appointments." The Health Secretary set out the following ambition for the:

> use of the best technology available for the NHS and social care sector. The potential of cutting-edge technologies to support preventative, predictive and personalised care is huge.
>
> For example, we could use more data-driven technologies such as artificial intelligence (AI) to help diagnose diseases or conditions and to gain better insights into treatments and preventions that could benefit all of society.[112]

NHSX was established in February 2019, and intends to deliver the Health Secretary's 'Tech Vision' and lead digital policy transformation through bring together the DHSC, NHS England and NHS Improvement. The NHS will help provide a framework for NHS organisations to share data and make commercial agreements with organisations in order to develop new technologies.

In July 2019 the Government also published a Code of conduct for data-driven health and social care technology and Guidance on creating the right framework to realise the benefits for patients and the NHS where data underpins innovation. This guidance stated that NHS organisations should not enter into agreements that grant one organisation exclusive right of access to raw NHS data, either patient or operational.

Recent use of patient data for planning and research with outside groups include:

- Moorfields/Deepmind – 1 million anonymised eye scans were shared with Deepmind under a research agreement that began in mid-2016. Deepmind's algorithm is designed to find early signs of age-related macular degeneration and diabetic retinopathy.
- John Radcliffe Hospital – worked with their partner, Ultromics, to use AI to improve detection of heart disease and lung cancer
- Imperial College London – researchers at Imperial and the University of Melbourne developed a new AI system that can predict the survival rates for patients with ovarian cancer

In September 2019, the Government stated that it was developing a set of tools to help technology sellers comply with principle 7 of the code of conduct, which stated that they should "show what type of algorithm is

[112] DHSC, 'Policy paper: the future of healthcare: our vison for digital, data and technology in health and care', 17 October 2018.

being developed or deployed, the ethical examination of how the data is used, how its performance will be validated and how it will be integrated into health and care provision."

Further reading on patient involvement in AI

Dame Fiona Caldicott appeared before the House of Lords Select Committee on AI in 2017. In answer to a question on the policy regulation of AI in the NHS, Dame Fiona Caldicott stated a desire for a review in relation to how the public are informed about the rights in relation to consent and use of anonymised data.[113] She stated that:

> We have quite a lot of education to do, not least with the professions that look after patients and with the public themselves, in explaining the benefits of this and giving reassurance that it is not going to be profit for companies they do not feel comfortable having access to their data, and making absolutely clear that this is safeguarded through anonymization and that it comes back into the national or public good.[114]

The think tank Reform's 'Making NHS data work for everyone' (December 2018) looks at how private sector companies access and use NHS data for research and development.

The All-Party Parliamentary Group on Heart and Circulatory Diseases, Putting patients at the heart of artificial intelligence (April 2019) called upon NHSX to set up discussions with charities, the public and others to better understand the views of patients regarding AI and the sharing of patient data.

On 5 September 2019 there was a Westminster Hall debate on the involvement of patients in the use of artificial intelligence in healthcare.[115] The Commons Library prepared a briefing ahead of this debate (CDP-2019-203, 30 August 2019).

On the 13 September 2019 a BMJ editorial stated that:

> …the public must be fully informed and proactively engaged in shaping decisions about how data are used and privacy protected. Commercial access to data remains a red line for some.[116]

5.1 Google DeepMind

In 2015, the company DeepMind, seeking to develop the "Streams" app that alerts of kidney injury, were given access by the Royal Free London NHS Foundation Trust to the previous five-years data of 1.6 million patients, most of whom had not had acute kidney injury.[117] The Trust was to receive free access to the app for five years in return for

---

113 House of Lords Committee on Artificial Intelligence: Oral Evidence, 21 November 2017, pp.17-18.
114 Ibid, p. 5.
115 HC Deb, Artificial Intelligence in Healthcare, vol 664, cc 154-175WH, 5 September 2019
116 'New AI laboratory for the NHS', British Medical Journal, 13 September 2019
117 'DeepMind Health received NHS data on inappropriate legal basis', *Digital Health*, 16 May 2017; 'Google AI has access to huge haul of NHS patient data', *New Scientist*, 29 April 2016.

sharing the data,[118] if the app did not provide more than £15,000 in support per month to the Trust.[119]

In addition to working with the Royal Free Hospital, DeepMind also worked with Moorfields NHS Trust from 2016.[120]

Dame Fiona Caldicott concluded in 2017 that data was improperly shared between the Royal Free NHS Trust and Google DeepMind. Patients are generally assumed to have implied consent to their medical records being shared for the purpose of their own "direct care." However, Caldicott stated that:

> Given that Streams was going through testing and therefore could not be relied upon for patient care, any role the application might have played in supporting the provision of direct care would have been limited and secondary to the purpose of the data transfer. My considered opinion therefore remains that it would not have been within the reasonable expectation of patients that their records would have been shared for this purpose.[121]

The Information Commissioner concluded that the Royal Free Trust failed to comply with the Data Protection Act of 1998 when it provided patient data to Google DeepMind.[122] In response, the NHS Trust asked the law firms Linklaters to audit the Trust's practices, and who concluded that the Royal Free's use of Steams was lawful, but offered recommendations to strengthen privacy and patient understanding, including considering an MoU between DeepMind and the Royal Free.[123] In July 2019, the Information Commissioner stated that the Royal Free Trust had completed its required actions and there were no further outstanding concerns on the current processing of personal data within "Streams."[124]

In August 2019, Dame Caldicott released NDG correspondence on the DeepMind inquiry, and stated that "my belief in innovation is coupled with an equally strong belief that these advancements must be introduced in a way that respects people's confidentiality and delivers no surprises about how their data is used."[125]

DeepMind is no longer a separate subsidiary of Google, and instead has become integrated into the company. The Independent Panel within DeepMind that scrutinised its work was also disbanded.[126]

---

118 House of Lords Committee Artificial Intelligence Committee, AI in the UK: ready, willing and able? (16 April 2017), para 286.
119 'Google DeepMind is giving the NHS free access to its patient monitoring app', Business Insider, 24 June 2017.
120 Moorfields NHS Trust, 'Latest Updates-DeepMind Health', 25 September 2019.
121 'NDG to the Royal Free NHS Trust', Sky News, 20 February 2017.
122 Information Commission, 'Royal Free- Google DeepMind trial failed to comply with data protection law', 3 July 2017.
123 Linklaters, 'Audit of the acute kidney injury detection system known as Streams' (May 2018), pp. 68-9.
124 Royal Free London NHS Foundation, 'Information Commissioner's Office (ICO) investigation' (September 2019)
125 NDG, 'Data driven innovation and meeting patients' reasonable expectations about data use', 23 August 2019.
126 'Google swallows DeepMind Health', BBC News, 18 September 2019.

In September 2019, Royal Free NHS Trust signed a new agreement with Google Health UK to continue work on the "Streams" app.[127] Imperial College Healthcare, Moorfields Eye Hospital and University College London NHS Trusts also signed a new agreement with Google Health UK for DeepMind technologies.[128] Taunton and Somerset NHS Trust signed a contract with Google, but no longer for the app. Yeovil District Hospital decided not to transfer an agreement over to Google Health.[129]

In answer to a PQ of December 2018, the Government said:

> **Lord O'Shaughnessy:** We have sought reassurance that none of the current contracts with National Health Service trusts will be transferred to Google, and any changes will require the agreement of the trusts. The patient data processed for Streams will remain controlled by the trusts, and will not be used for any purpose other than the provision of direct patient care, as specified in existing agreements.
>
> We are working with DeepMind and Google as they consider how to provide assurance on the use of patient data as Streams grows into a global product. The Code of Conduct for Data Driven Technologies sets out the principles that we expect NHS trusts and industry partners to follow.[130]

In answer to a separate PQ, the Government additionally stated:

> **Lord O'Shaughnessy:** We will seek a full explanation from Google about its plans, including why they have halted the independent review panel and how they intend to replace this function.
>
> We will work with regulators, including the Information Commissioner's Office, and the Centre for Data Ethics and Innovation to ensure anything that happens as a result of the transfer of Streams respects patients' privacy and complies fully with the law.
>
> I met with DeepMind recently and raised this issue with them.[131]

In September 2019, the UK Site Lead for Google Health, Dr Dominic King, wrote:

> Health data is sensitive, and we gave proper time and care to make sure that we had the full consent and cooperation of our partners. This included giving them the time to ask questions and fully understand our plans and to choose whether to continue our partnerships. As has always been the case, our partners are in full control of all patient data and we will only use patient data to help improve care, under their oversight and instructions.[132]

---

127 Royal Free NHS Trust, 'Our work with Google Health', 31 July 2019
128 Imperial College Healthcare NHS Trust, 'Trust updates technology partnership to continue improvements to patient care', 18 September 2019.
129 'NHS Trusts sign first deals with Google', Financial Times, 19 September 2019.
130 PQ, HL12329, DeepMind, 14 December 2018
131 PQ, HL11728, DeepMind, 22 November 2018
132 Dominic King, 'DeepMind's health team joins Google Health', Google Blogs, 18 September 2019.

5.2 Amazon Alexa

In July 2019, the NHS website team worked with Amazon to make available medical advice over the voice-assisted Amazon Alexa. The NHS stated that no information collected by Amazon would be shared with third parties, build a health profile, or sell or recommend products. The Minister for Culture, Media and Sport stated that:

> **Margot James**: No patient data held by NHS bodies is being shared by Amazon. The agreement is clear that Amazon will not share information with third parties, nor is it going to sell products, make product recommendations or build a health profile on users.[133]

Because the information provided by Alexa is based on the NHS Website and intended to improve accessibility of NHS advice, Amazon has not paid the NHS for the service. The NHS also confirmed it was in talks with other providers beyond Amazon.[134] In January 2020, the Government has said this agreement is not exclusive, and that there were 2,000 other organisations accessing and using information "from the National Health Service website in a similar way".[135]

In response to an FoI, a redacted version of the contract signed between Amazon and the Secretary of State for Health and Social Care, was published by the DHSC in October 2019.[136] The DSHC said that some information was redacted from publication under the Freedom of Information Act for being "likely to prejudice the commercial interests of Amazon" by "harm[ing] Amazon's negotiating position when entering into agreements with other parties in the future" and potentially leading to the challenging of existing agreements that Amazon had with other parties.[137]

5.3 Telefonica

For a six-month pilot between November 2018 and May 2019, the telecoms company Telefonica, which owns O2, was given access to certain NHS medical records to develop an algorithm aimed at predicting when mental health crises might occur.[138]

The project was funded by a £1.8 million grant from NHS England and data came from Birmingham and Solihull Mental Health NHS Foundation Trust.

The Times newspaper reported the Foundation Trust as stating "there is no reason for our patients to be concerned in any way about how their information is being used" and that the Trust would consult with the

---

133 PQ, 275709, NHS: Amazon, 10 July 2019.
134 NHS Digital, 'How we are talking to Alexa', 25 July 2019
135 PQ, HL126, NHS: Amazon, 7 January 2020
136 'Government Hands Amazon Free Access to NHS Information', BMJ, 9 December 2019.
137 DSHC to Mr Sam Smith, Freedom of Information Request FOI-1182708, 31 October 2019.
138 Birmingham and Solihull Mental Health Trust Board of Directors Papers (Public) October 2019, 29 October 2019, pp. 48-9

Information Commissioner's Office before proceeding further. Patients would have the ability to opt out in any roll-out of the algorithm.[139]

In answer to an oral question in the Lords, the Minister Lord Bethell stated that "the data has not left the servers of the Birmingham and Solihull Trust and it is not being used outside the remit of the pilot arranged by that project".[140]

5.4 Coronavirus data store

In March 2020, NHS England & Improvement announced they would create a data store to bring multiple data sources related to coronavirus outbreak into a single location. Data will come across the NHS and include metrics such as hospital occupancy and information about the length of stay for Coronavirus patients.

Private companies, including Microsoft, Palantir Technologies, Amazon Web Services, Faculty and Google, are involved in different aspects of the project. NHS England state that all data entered is anonymised and only used for Coronavirus purposes. It also says that "our technology partners are subject to the same strict rules for information governance that we follow in our day to day work".

Once the Coronavirus outbreak is contained, NHS England says that "data will either be destroyed or returned in line with the law and the strict contractual agreements that are in place between the NHS and partners."[141]

The Guardian reported on 12 April 2020 that it had seen documents appearing to show that "large volumes of data pertaining to individuals, including protected health information, Covid-19 test results, the contents of people's calls to the NHS advice line 111 and clinical information" were also included in the data, although anonymised. Faculty, one of the companies involved, told the Guardian that they had access to only aggregated or anonymised data.[142]

5.5 Coronavirus-tracing app

On 18 March 2020, NHSX, a Government body responsible for setting national policy on technology within the NHS, stated it was working on a contact tracking app to trace the spread of coronavirus through the population.[143] The BBC reported the response of Oxford University academics who published an article in the Journal Science on using an app to record people's GPS location data to monitor the virus. The academics noted that they were currently exploring whether an app

---

139 'NHS medical records given to telecoms group to predict mental breakdowns', The Times, 26 January 2020
140 HL Deb, NHS Data, vol. 801, c 1328, 28 January 2020
141 Technology in the NHS, 'The power of data in a pandemic', 28 March 2020
142 'UK government using confidential patient data in coronavirus response', The Guardian, 12 April 2020
143 'NHS developing coronavirus contact tracking app', Health Service Journal, 18 March 2020

would be effective if it relied on people using a questionnaire or NHS 111 helpline advisers to diagnose the virus, instead of a test.[144]

Appearing before the Health and Social Care Committee on 5 March 2020, the Chief Medical Officer for England, Chris Whitty, in response to a question referencing the South Korean app able to provide the location of someone with coronavirus, said:

> I am very against giving any patient-identifiable information, and for that reason we should also be careful, so I am not in favour of going down to street level or, "You are within 100 metres of coronavirus." That is the wrong approach for this country.[145]

On 12 April 2020, the Secretary of State for Health and Social Care said that a new NHS tracking app was already being tested. He said that:

> If you become unwell with the symptoms of coronavirus, you can securely tell this new NHS app.
>
> And the app will then send an alert anonymously to other app users that you've been in significant contact with over the past few days, even before you had symptoms, so that they know and can act accordingly.
>
> All data will be handled according to the highest ethical and security standards, and would only be used for NHS care and research.
>
> And we won't hold it any longer than is needed.[146]

The Guardian reported that NHS England was shown a memo in March 2020 that the app could use device IDs, enabling de-anonymisation if Ministers judged this proportionate. However, NHSX stated that "there have never been plans to make use of existing apps and other functions already installed on peoples phones such as Google Maps and neither have there been plans to look to use the device ID of users in any app-based solutions."[147]

Appearing before the Science and Technology Committee on 28 April 2020, Matthew Gould, the Chief Executive of NHSX, said that the app would have

> identifiers rather than identities, which sit on people's phones until they choose to share it with us. So there are a series of protections that allow people to be confident in using it that their privacy is being protected. [148]

On the Technology in the NHS blog, he also said:

> The data will only ever be used for NHS care, management, evaluation and research. You will always be able to delete the app and all associated data whenever you want. We will always comply with the law around the use of your data, including the Data Protection Act and will explain how we intend to use it. We will be totally open and transparent about your choices in the app and what they mean. If we make any changes to how the app

144 'Coronavirus: UK considers virus-tracing app to ease lockdown', BBC News, 31 March 2020
145 Health and Social Care Committee, Preparations for coronavirus, 5 March 2020, Q5
146 No10 YouTube Channel, Coronavirus Press Conference, 12 April 2020, from 9:19
147 NHS Coronavirus app: Memo discussed giving ministers power to 'de-anonymise' users, The Guardian, 13 April 2020
148 Parliament.TV, Science and Technology Committee, 28 April 2020, at 10:33

works over time, we will explain in plain English why those changes were made and what they mean for you. Your privacy is crucial to the NHS, and so while these are unusual times, we are acutely aware of our obligations to you. Just as the NHS strives at all times to keep your health records confidential, so it will keep the app data secure. Patient confidentiality is built in to the NHS. It is one of our key values.

[…]

We have worked quickly to build the app because that is what the situation demands. But we have not let that urgency compromise our commitment to transparency, ethics and the law. We have been consulting on our plans with the Information Commissioner (see this blog), the National Data Guardian's Panel and the Centre for Data Ethics and Innovation, as well as with representatives from Understanding Patient Data and volunteers who provided a patient and public perspective. We have established an ethics advisory board for the app, chaired by Professor Sir Jonathan Montgomery from University College London who previously headed the Nuffield Council on Bioethics. Their advice and expertise will be crucial to everything we do.[149]

[149] Matthew Gould and Geraint Lewis, Digital contact tracing: Protecting the NHS and saving lives, 24 April 2020

6. Cross-border data sharing after Brexit

6.1 Patient Data in Trade Agreements

The House of Commons Library Debate Pack on 'Future trade deals and the National Health Service' (July 2019) examines the debates over the effect on future trade agreements on the NHS.[150] This section relates only to the treatment of NHS patient data. Data held by the NHS was estimated by Ernst & Young to be worth £9.6 billion a year, including £4.6 billion of benefit to patients through personalised care and data initiatives.[151]

6.2 US-UK Trade Agreement

In the United States-United Kingdom Negotiations Paper of February 2019, the United States Trade Representative stated that one negotiating objective of the United States was to:

> Establish state-of-the-art rules to ensure that the UK does not impose measures that restrict cross-border data flows and does not require the use or installation of local computing facilities.

Further documents, released by the Labour Party on 27 November 2019, outlined 6 meetings held between US Trade Representatives and the UK Department for International Trade from July 2017 to July 2019, confirming an interest of the US trade representative in "obtaining commitments on the free flow of data [as] a top priority".[152]

In a July 2019 Westminster Hall debate on a petition relating to future trade deals and the NHS, the Minister for Trade stated that:

> I guarantee the House that the Government will protect the NHS in trade negotiations. That means no requirement to increase private provision, no allowing American companies to ramp up drug prices, and no undermining the safeguards on healthcare data.
>
> […]
>
> The Government will ensure that trade negotiations do not undermine the safeguards that we have in place around health and care data. Those safeguards allow the public to have trust in how and why their data is used, and it is incredibly important that we maintain them.
>
> To be clear, free trade agreements of course have a role in data. At the Department for International Trade, we are tasked with ensuring that data flows on a legal, safe and secure basis. We would seek to review any rules in place to safeguard data, such as data localisation requirements, and ensure that they are not overly protectionist. However, that should not be confused with the data

[150] The House of Commons Library Debate Pack 'Outsourcing and privatisation in the NHS' (May 2018), provides more detail on the role of private providers in the NHS.
[151] Ernst & Young, 'Realising the value of health care data: a Framework for the future' (July 2019), p.3.
[152] 'US Could Get Access to UK Health Data, Experts Warn', BMJ, 3 December 2019.

> that actually flows. We set up the pipework, but whether or not the taps are turned on is a matter for the regulators. In our case, that is the Information Commissioner's Office, which is entirely clear about the need for privacy and cyber-security.[153]

A debate was also held in the House of Lords on the place of the NHS in any trade agreement following Britain's departure from the EU in July 2019.

The EU-US Privacy Shield currently allows data sharing between the EU, Switzerland and the USA, if US-based organisations comply with the framework's requirements. In response to a PQ, the then-Health Minister Baroness Blackwood stated that:

> As the United Kingdom leaves the European Union we have made arrangements with the United States that will ensure that in both 'deal' and 'no deal' scenarios, transfers of personal data from the UK to US Privacy Shield participant organisations can continue to be made under the Privacy Shield Framework.[154]

The Information Commissioner has stated that if the UK leaves the EU without a withdrawal agreement, personal data will only be able to transferred to US organisations participating in the Privacy Shield if they have updated their privacy commitments to state that they also apply to the UK.[155]

6.3 Sharing Patient Data with the EU post-Brexit

The *Data Protection, Privacy and Electronic Communications (Amendments etc) Regulations 2019* state that following the UK's exit from the EU, the same standards on data flow will be enforced, with the Secretary of State having the power to determine whether third-countries can be granted "adequacy status" to enable data transfers. The UK has legislated to continue the free flow of personal data from the UK to the EU/EEA on a transitional basis, and the Government intends to keep this under review.[156] The EU Commission has yet to confirm whether it will award the UK "adequacy status" for the purposes of data sharing.[157]

NHS England has published details on preparing the NHS for continuity of access to process and sharing data as part of the Government's contingency preparations for a 'No-deal' Exit from the EU, and wrote to NHS Data Protection officers in February 2019. Potential delays in the sharing of patient data have seen concerns raised in Northern Ireland,[158] and for Irish citizens who potentially access NHS treatment in the rest of

---

153 HC Deb, NHS and Future Trade Deals, vol. 663, cc 492-3WH, 22 July 2019.
154 PQ, HL17043, Data Protection: USA, 9 July 2019
155 Information Commission's Office, 'International data transfers' (accessed 7 October 2019).
156 HM Government, No-deal readiness report (October 2019), p. 53.
157 Ibid, pp. 52-6.
158 'Patients on both sides of Irish border face medical risks in no-deal Brexit', Politico, 27 August 2019.

the UK (1,991 applications being made to do so in England from 2015 to 2017).[159]

[159] 'Republic of Ireland set to be the biggest loser if no deal struck on European healthcare schemes', The Detail, 7 November 2018.

BRIEFING PAPER
Number 07103, 28 April 2020

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publically available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcinfo@parliament.uk.

Disclaimer