House of Commons Library

Research Briefing

By Aaron Kulakiewicz,
Tom Powell

8 July 2022

Patient health records: Access, sharing and confidentiality

Contributing Authors
Elizabeth Parkin

Image Credits
And you haven't been to your doctor because? By Alex Proimos. Licensed under CC BY 2.0 / image cropped.

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

If you have any comments on our briefings please email papers@parliament.uk. Please note that authors are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

You can read our feedback and complaints policy and our editorial policy at commonslibrary.parliament.uk. If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk.

Contents

Summary

Accessing personal health records

Individuals have a right to access their own health records and in limited circumstances, to access information about other people. Since 25 May 2018 this has been governed by the Data Protection Act 2018. Record holders cannot charge patients for accessing records, the exception to this is where requests are "manifestly unfounded or excessive". In these cases, the data controller can charge a fee to cover administrative costs or refuse to act on the request. There are also certain circumstances in which full access to a patient's health record may be denied, such as where the release is likely to cause serious harm to the physical or mental health of the individual or another person.

Accessing someone else's health records

Children aged 12 or over are generally expected to have capacity to give or withhold consent to the release of information. However, the guidance says every reasonable effort must be made to persuade the child to involve parents or guardians. A deceased patient's health records are still protected under the Access to Health Records Act 1990 and someone will only be entitled to access a deceased person's records if they are either a personal representative of the patient or have a claim resulting from the death.

Sharing confidential patient information

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. Patients have the right to privacy and confidentiality and to expect the NHS to keep their confidential information safe and secure. Patients also have the right to request that their confidential information is not used beyond their own treatment. The Health and Care Act 2022 includes measures relating to the collection and sharing of health and care data.

It should be noted that there are exceptional circumstances in which a health or social care professional may be obliged to share confidential patient information in line with the "public interest" or when they are required by law to disclose medical information, regardless of a patient's consent.

For the most part, the law on confidentiality applies in the same way to patients detained under the Mental Health Act 1983 as to any other type of patient. However, under the Act, there are some situations, such as to manage serious risks, where information can be shared without the patient's consent. Also, if a patient lacks mental capacity to give or withhold their consent medical information may need to be shared with relatives, friends and carers to enable health professionals to determine their best interests.

Electronic health records

Since 2014 the NHS has committed to making patient records largely paperless with the introduction of various online records. The initial target for this transition was 2020 but this was pushed back to 2023. In February 2022, the then Secretary of State for Health and Social Care, Sajid Javid, set a target for 90 per cent of NHS trusts to use Electronic Patient Records (EPRs) by the end of 2023, with the remaining 10 per cent needing to be in an 'implementation phase'. The NHS has created various electronic records, these include:

- Summary Care Records (SCRs) are electronic health records containing essential information about a patient, such as their medication and allergies.

- Shared Care Records are the new term for Local Health and Care Records which enable the safe and secure sharing of an individual's health and care information as they move between different parts of the NHS and social care.

NHS data and cyber security

The National Data Guardian (NDG) for health and care undertook a review of NHS data security in 2016 which set out a number of recommendations to improve cyber security. In the wake of the 2017 WannaCry cyber attack, which impacted on 80 of the 236 NHS Trusts in England and is estimated to have cost the NHS £92 million, the Government accepted the Review's recommendations. In 2018, the Government launched the Data Security and Protection Toolkit to implement the data security standards.

Patient data, Apps and Artificial Intelligence (AI)

In June 2022 the Government published a strategy, Data saves lives, setting out the Secretary of State's vision for how patient data should be used "to

bring benefits to all parts of health and social care" and to "demonstrate that the health and care system is a trustworthy data custodian". The strategy also makes reference to patient involvement in AI in health and care.

The NHS App was launched on 31 December 2018 and at 31 December 2021 it had over 22 million users. The Government committed to continue to develop the NHS App so 75% of the adult population will be registered to use it and the NHS website by March 2024. Additionally, individuals can access a digital version of their Covid-19 vaccination status in two ways, either by using the NHS App or the NHS COVID Pass service.

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 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 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 General Data Protection Regulation (GDPR), enacted by the Data Protection Act (DPA) 2018. This legislation repealed the Data Protection Act 1998. In 2010, the Department of Health produced Guidance for Access to Health Records Requests. This sets out the legislative basis for patients' access to health records in other circumstances, 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]

NHS Digital has published a webpage, General Data Protection Regulation (GDPR) - information, which provides an overview on how the NHS ensures compliance with data protection law and makes sure health and care data is always collected, stored, analysed and shared securely and legally.

Under the DPA 1998, an individual had to request access to their health record in writing, although the earlier guidance said requests could be made verbally where a patient was unable to submit a written request.[3] The 2018 data protection legislation does not specify ways in which requests for access have to be made.[4]

1 NHS England, 'How do I get a copy of my health (medical) records?' (accessed 10 March 2022).
2 Department of Health, Guidance for Access to Health Records Requests (February 2010), p8.
3 Department of Health, Guidance for Access to Health Records Requests (February 2010), p9.
4 NHS England, 'How to access your personal information' (accessed 10 March 2022); Information Commissioner's Office, Preparing and submitting your subject access request (accessed 10 March 2022).

The GDPR also reduced the period within which requested medical records must be provided from 40 days to one month.[5] In earlier guidance (2010), the Government made a commitment that health record requests should normally be handled within 21 days, despite the longer legal time limit under the 1998 DPA.[6]

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.[7] NHS organisations should retain records in accordance with the retention schedules outlined in Appendixes II and III of the 2021 NHSX publication, Records Management Code of Practice 2021.

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. 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".[8] In these cases, the data controller can charge a reasonable fee to cover 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.

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.[9] The 1988 Act allows GPs to charge reasonable fees for these reports.[10]

1.2 Limiting patient access to their health records

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

5 Medical Protection, The General Data Protection Regulation (GDPR), (April 2018)
6 Department of Health, Guidance for Access to Health Records Requests (February 2010), p10
7 Records Management Code of Practice 2021, Appendix II.
8 Data Protection Act 2018, Chapter 2, Section 12.
9 Association of British Insurance, Access to Medical Records
10 Access to Medical Reports Act 1988, Section 4(4).

- 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.[11]

Where records 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.[12]

1.3 Parental access to child health records

The British Medical Association (BMA) has produced guidance on the care of children and young people, which includes advice on confidentiality and the disclosure of health records. This guidance says that children aged 12 or over are generally expected to have capacity to give or withhold consent to the release of information, and are legally assumed to have capacity when aged 16 or over in England, Wales and Northern Ireland.[13] In Scotland, anyone aged 12 and over is legally presumed to have competence to give or withhold consent.[14]

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

> **When is a young person competent to consent to the disclosure of their personal information?**
>
> [...]

11 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.

12 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.

13 PQ. HL15330, Medical Records: Children, 07 May 2019

14 British Medical Association (BMA), Children and young people ethics toolkit (accessed 2 April 2020), p16.

Health professionals should, unless there are convincing reasons to the contrary, eg, abuse is suspected, respect the child's wishes if they do not want parents or guardians to know about all or some aspects of their healthcare (see section 15 on child protection). However, every reasonable effort must be made to persuade the child to involve parents or guardians particularly for important or life-changing decisions.

Are there limits to confidentiality if a child lacks competence?

Occasionally, children who lack competence seek or receive healthcare without their parents or guardians being present. They may lack the competence to give consent to treatment, and the disclosure of information (see section 13, for example, on sexual activity). In these circumstances, confidentiality should usually be respected if they share information on the understanding that the information will not be disclosed to parents or guardians, or indeed to any third party. Parental involvement, however, should be encouraged, unless there are very convincing reasons to the contrary. [15]

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)

Access to a deceased person's health records may not be granted if the patient requested confidentiality whilst they were alive. No information can be revealed if the patient requested non-disclosure.[16]

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.[17]

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

[15] As above, p16.
[16] Access to Health Records Act 1990, (PDF) Chapter 23, 4(3)
[17] Access to Health Records Act 1990, (PDF) Chapter 23, 5(1)(a)

2 Sharing confidential patient information

The sharing of anonymised patient information more widely has potential to 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 suitably anonymised and untraceable to individuals before it is released.[18]

2.1 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 confidential patient information safe and secure, and the right to be informed about how their information is used.[19]

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.[20]

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 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 health records toolkit says:

> Confidentiality is essential to the relationship of trust between doctors and patients. The principles of confidentiality apply to all doctors irrespective of their speciality. Patients must be able to expect that information about their health which they give in confidence will be kept confidential unless there is a compelling reason that it should not be.[21]

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

19 NHS England, Patients and the public: your rights and the NHS pledges to you; NHS Constitution for England, January 2021

20 As above

21 BMA, Confidentiality and health records toolkit (accessed 5 May 2022), p1.

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 (PDF) introduced a legal duty for health and social care professionals to share patient information where they consider 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:

> 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.[22]

The Health and Care Act 2022, which received Royal Assent on 28 April 2022, includes measures relating to the collection and sharing of health and care data. These provisions are intended to enable increased sharing and more effective use of data across the health and adult social care system.

Specifically, the legislation aims to enable the Department of Health and Social Care and NHS England to publish mandatory information standards to ensure providers of health and adult social care adopt a standardised approach to the collection and processing of data. These provisions extend the potential application of information standards to include private providers of health and adult social care. The Government has said it wants to see more effective use of data, to support individuals and the wider health and care system:

> Building on the successful data sharing in response to COVID-19, we want to ensure that health and care organisations use data, when they can do so and with appropriate safeguards, for the benefit of individuals and the wider health and social care system. The forthcoming Data Strategy for Health and Care will set out a range of proposals to address structural, cultural/behavioural and legislative barriers to data sharing and a more flexible legislative framework to improve data access and interoperability, including enabling the safe sharing of data in support of individual care, population health and the effective functioning of the system.[23]

2.2 NHS Digital guidance on confidentiality

The Health and Social Care Act 2012 (PDF) 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

---

22 BMA evidence to the Health and Social Care (Safety and Quality) Bill House of Lords Committee stage, (PDF) 13 March 2015, pp1-2.

23 Gov.uk, Integration and innovation: working together to improve health and social care for all, February 2021

and other dissemination of confidential information concerning, or connected with the provision of health services or of adult social care in England."[24]

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

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[25]

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

2.3 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 Data Guardian) Act 2018 placed the role on a statutory footing.[26] The 2018 Act means 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

[24] Health and Social Care Act 2012 (PDF), 13S (1)

[25] HSCIC, A guide to confidentiality in health and social care (September 2013), p3. The guide is supported by a references document (September 2013) which provides more detailed information for organisations and examples of good practice.

[26] 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).

the NHS or publicly funded adult social care. In March 2019 Dame Fiona was confirmed as NDG, a position she held until her death in February 2021.[27] Dr Nicola Byrne is the current NDG, having been appointed in March 2021.[28]

The NDG's terms of reference set out 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.[29]

Caldicott principles

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

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

27 NDG, Dame Fiona Caldicott tribute, 15 February 2021
28 NDG, Dr Nicola Byrne to be the National Data Guardian for Health and Social Care, 19 March 2021
29 NDG, Progress Report: January 2018-March 2019 (PDF), 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 (PDF) in September 2013, and accepted in principle each of the 26 recommendations. The Government's response outlined how these recommendations would be implemented, and included key commitments for health and social care providers, NHS England and organisations such as the Care Quality Commission (CQC).

2.4 National data opt-out programme

On 25 May 2018, NHS Digital launched the national data opt-out programme, a tool which allows patients 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.[30]

The national programme is replacing the system of Type 1 and Type 2 opt-outs (as well as a number of local opt-out systems).[31] Type 2 opt-outs, where patients registered with their GP to prevent their information being shared

30 NHS Digital, 'National data opt-out'

31 NHS Digital, 'Opting out of sharing your confidential patient information', 20 August 2021.

with organisations outside the NHS, are being automatically converted to the national data opt-out programme. Patients are being informed about this individually.[32]

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 the Department of Health and Social Care (DHSC) conducts a consultation with the NDG on their removal.[33]

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 repeatedly extended, and is now set for 31 July 2022.[34]

As of September 2021, 5.35% of registered patients had an active national data opt-out, 3.26 million patients.[35] This compared to 1.6 million in July 2018.[36]

The national data opt-out system is based on a recommendation by the NDG, in the 2016 Review of Data Security, Consent and Opt-Outs (PDF). The review was launched following the suspension of the national Care.data programme, due to concerns over the opt-out system and over patient confidentiality.[37] Following the review, the then-Life Sciences Minister George Freeman confirmed in July 2016 that Care.data would be closed.[38]

The Government's response to the NDG review (PDF) confirmed 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 (PDF).

2.5 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 a patient's consent. For example, statutory disclosures are required under the following legislation, although this is not an exhaustive list:

32 NHS Digital, 'Collection and conversion of type 2 opt-outs', 7 March 2019.
33 NHS Digital, 'Information for GP practices', 30 March 2022.
34 NHS Digital, 'National data opt-out' ; NHS Digital and NHSX to NHS England, (PDF) 19 March 2020
35 NHS Digital, 'National Data Opt-Out, September 2021'
36 NHS Digital, 'National Data Opt-Out, July 2018'
37 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).
38 Care Quality and National Data Guardian for Health and Care's Independent Reviews into Data Security, HCWS626 July 2016

- 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. Under section 261 of the Health and Social 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 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 not directly related to a patient's care.[39]

2.6 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.

[39] HSCIC, A guide to confidentiality in health and social care, September 2013, p21.

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.[40] In light of these concerns, in January 2018, the then Chair of the Health Select Committee, Dr Sarah Wollaston, wrote to NHS Digital requesting they withdraw from the MoU.[41] A subsequent letter to the Committee from the Government noted these concerns, but argued there was no cause for a significant change of approach.[42]

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.[43]

In response, the then Digital and Creative Industries Minister, Margot James, announced a change in approach in 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.[44]

Dr Wollaston's amendment was withdrawn. On 28 January 2019, the DHSC, the Home Office and NHS Digital said "they will continue to work together to agree how future information requests will be processed."[45] Public Health England conducted a review on the potential impact of a new MoU on public health, ending in April 2019.[46] The webpage notes that Public Health England are analysing feedback.[47]

---

40 Health Committee, Correspondence regarding memorandum of understanding between NHS Digital, Home Office and the Department for Health on data sharing (PDF), 2017, 'PHE Response: February 2017', p1.

41 Health Committee, Letter to Sarah Wilkinson, Chief Executive, NHS Digital, regarding sharing of patient address information with the Home Office for immigration enforcement purposes, (PDF) 29 January 2018.

42 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, (PDF) 23 February 2018.

43 HC Deb Data Protection Bill (Lords), vol. 640, c 770, 9 May 2018

44 HC Deb Data Protection Bill (Lords), vol. 640, cc 756-8, 9 May 2018

45 DHSC, 'Information requests from the Home Office to NHS Digital', 28 January 2019.

46 PQ 211731, Health Services: Immigrants, 23 January 2019

47 Public Health England, 'Data sharing MoU between NHS Digital and Home Office' (accessed 9 June 2022).

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 agreed.[48]

Data sharing between the NHS and the Home Office concerning patients subject to immigration rules with a total NHS debt of over £500 was unaffected by the MoU's withdrawal.[49]

2.7 Public interest disclosures of patient information

There are 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 as:

> A disclosure of confidential information because it is in the 'public interest' can be justified if it is essential to:
>
> – prevent, detect or prosecute serious crime;
>
> – prevent a serious threat to public health or national security;
>
> – or to protect individuals or society from serious harm.[50]

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.[51]

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:

> 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.[52]

48 Coronavirus Bill: Committee of the Whole House, 23 March 2020
49 DHSC, Overseas chargeable patients, NHS debt and immigration rules (PDF), 26 March 2019.
50 BMA, Confidentiality and health records toolkit (accessed 5 May 2022), p14.
51 HSCIC, A guide to confidentiality in health and social care, September 2013
52 HSCIC, A guide to confidentiality in health and social care, September 2013, section 8.

2.8 Deceased patients

There is an ethical obligation to respect a patient's confidentiality after death. 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.[53] The Department of Health and Social Care, General Medical Council (GMC) and other clinical professional bodies have long accepted that the duty of confidentiality continues beyond death and this is reflected in their guidance.[54]

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 (ie 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).[55]

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.[56]

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

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

53 BMA, Access to health records (June 2019), p9.
54 Department of Health, Guidance for Access to Health Records Requests (February 2010), p13.
55 Access to Health Records Act 1990, (PDF) Chapter 23, 4(3)
56 Access to Health Records Act 1990, (PDF) Chapter 23, 5(1)(a)

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.[57]

[57] General Medical Council, Ethical Guidance for Doctors: 'Managing and Protecting Personal Information' (last accessed 12 April 2022).

2.9 Assessment of capacity to give or withhold consent

If a patient lacks mental capacity to 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:

> 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.[58]

In England and Wales, decisions about mental capacity are governed by the Mental Capacity Act 2005 (MCA). Patients who have a mental health condition or a learning disability do not automatically lack capacity. Capacity assessments should be decision specific, so a person who lacks capacity to make a decision about treatment may have capacity to consent to their information being shared with a professional or relative.

Where a person does not have capacity to make a decision, access to information about them may be required to make a decision in their best interests.[59] This could include sharing relevant information with a legally appointed proxy decision maker, a carer, or, if there is no one else to consult, an Independent Mental Capacity Advocate (IMCA).[60]

2.10 Information sharing under the Mental Health Act

For the most part, the law on confidentiality applies in the same way to patients detained under the Mental Health Act 1983 as to any other type of patient. However, under the Act, there are some situations where information can be shared without the patient's consent. These include reports to the Tribunal or Care Quality Commission, to manage serious risks or ensure the safe transfer a patient.[61] The Act also requires that Nearest Relatives are given a copy of any information given to the patient and informed of their

58 British Medical Association, Confidentiality and health records toolkit, July 2021, p8.
59 See Office of the Public Guardian, Mental Capacity Act Code of Practice, Chapter 16
60 See Office of the Public Guardian, Mental Capacity Act Code of Practice, Chapter 10
61 Department of Health, Code of practice: Mental Health Act 1983, January 2015, Chapter 10.

discharge from detention (or CTO). The patient can object to the sharing of all or some of this information.[62]

Under the Act, qualifying patients are entitled to support from an Independent Mental Health Advocate (IMHA). With the patient's consent, IMHAs may inspect any records relating to the patient's detention or treatment in any hospital, or to any after-care services. If the patient lacks capacity to consent, the IMHA may be allowed access if the disclosure of information is in the patient's best interests. [63]

The Government's White Paper Reforming the Mental Health Act (January 2021) proposes to introduce a new Nominated Person (NP), replacing the current Nearest Relative role:

> The review highlighted that service users and stakeholders consistently found the current model of family and carer involvement is outdated and insufficient. This was found to be particularly true of the current Nearest Relative (NR) provisions.
>
> The Nearest Relative has a specific set of rights and powers in relation to the patient. The Act includes a prescribed list which is used to determine the person who is given this role, and therefore the patient has no say in who it is who will take on these specific rights and powers. This can sometimes mean that patients are assigned an inappropriate Nearest Relative, who is not best placed to support their needs. In some instances, this can compound what is already a distressing time and even retraumatise people particularly where they have experienced gender-based violence. As recommended by the review, we will seek to replace the Nearest Relative with a new statutory role, known as the nominated person, who the patient can personally select to represent them.[64]

The planned introduction of statutory Advance Choice Documents will also allow patients to make decisions on the sharing of information prior to detention under the Act or loss of capacity.[65] More information on the reforms to the Mental Health Act can be found in the Library Briefing on The White Paper on Reforming the Mental Health Act. A draft Bill is expected in the 2022-23 parliamentary session.

2.11 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, which inserted section 251B of the Health and Social Care Act 2012. This provides a duty for information to be shared where it facilitates care for an individual and it is

62 As above, Chapter 4.
63 Ibid., paras 6.30 to 6.38.
64 Department of Health and Social Care, Reforming the Mental Health Act, January 2021, p49.
65 As above, p35.

legal to do so. The patient must be informed and be provided with an opportunity to object. The Act followed the 2013 Caldicott Review.

The PQ reproduced below from 2016 explains that private sector providers contracted to provide direct care to NHS patients are expected to share and receive patient information for the 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.[66]

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

> 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.[67]

66 PQ. 37056, Medical Records: Disclosure of information, 24 May 2016

67 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, then-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.[68]

NHS England's Five Year Forward View (5YFV; October 2014), committed to making all patients' records "largely paperless" by 2020. The 5YFV committed the National Information Board to publishing plans to develop fully interoperable electronic health records so patients' records are largely paperless. Patients would have full access to these records and be able to write into them. They would retain the right to opt out of their record being shared electronically. The NHS number, for safety and efficiency reasons, would be used as an identifier in all settings, including social care.[69]

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 (PDF). 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 said:

---

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

69 NHS England, Five Year Forward View, (PDF), October 2014.

> 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.[70]

As of January 2017, all local health and care systems had produced Local Digital Roadmaps, setting out how they would achieve the ambition of 'paper-free at the point of care' by 2020.[71]

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 use and potential benefits of electronic health records, and challenges to implementation, including IT systems, data security and privacy

Revised Timescale

A Government commissioned review of NHS IT by Robert Wachter reported in September 2016. It said 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.[72]

Then-Health Secretary, Jeremy Hunt, supported the revised timetable for digitising the NHS.[73] 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 (PDF), published in January 2019, said all providers, across acute, community and mental health settings, would 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.
- 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.

---

70 As above, p29.

71 NHS England, Local Digital Roadmaps

72 Making IT Work: Harnessing the power of health information technology to improve care in England, 7 September 2016

73 National Health Executive, 'NHS IT, records and data', 8 September 2016.

- 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.[74]

In February 2022, the Secretary of State, Sajid Javid, set a target for 90 per cent of NHS trusts to use Electronic Patient Records (EPRs) by the end of 2023, with the remaining 10 per cent needing to be in an 'implementation phase'.[75]

In May 2022, the Health Service Journal reported Rory Deighton, acute lead at NHS Confederation, as saying NHS Trusts' efforts to roll out EPRs had often been "hampered by inadequate levels of available capital funding". He said the upcoming NHS digital health plan should "commit to providing leaders with the necessary support to roll out comprehensive EPR systems".[76]

3.2 Summary Care Records

Summary Care Records (SCRs) are electronic health records containing essential information about a patient, such as their medication, allergies and adverse reactions. NHS Digital notes that SCRs are created from GP medical records and can be seen and used by authorised staff in other areas of the health and care system involved in the patient's direct care.[77]

The NHS Digital webpage 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)

74 NHS England, NHS Long Term Plan (PDF), January 2019, pp96 &99.
75 Speech by Health and Social Care Secretary Sajid Javid at the HSJ Digital Transformation Summit, 24 February 2022
76 Health Service Journal, Revealed: The 28 trusts still without an electronic patient record, 26 May 2022
77 NHS Digital, Summary Care Records (SCR)

- 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)[78]

A reasonable adjustment 'digital flag' will also be added to the SCR by 2023/24 in order to alert NHS staff of patients with a learning disability or autism.[79] Patients can choose to include additional information, such as long-term conditions and specific communication needs.

Health and care professionals must have a smartcard with the correct codes to access an SCR. All usages must be logged, and a patient can 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.[80]

First introduced in 2010, as of December 2017, 98% of the population in England had a SCR, and were estimated to be used around 6.5 million times.[81]

3.3 Shared Care Records

NHS England has said it is investing in a number of Local Health and Care Record Exemplars to enable the safe and secure sharing of an individual's health and care information as they move between different parts of the NHS and social care.[82] NHS England and the Local Government Association published a briefing in 2018 with further detail on a number of the Local Health and Care Record Exemplars.

In February 2022, NHSX (now part of the NHS Transformation Directorate) published information on what it referred to as "Shared Care Records", as the new term for Local Health and Care Records.[83]

The Government's white paper Health and social care integration: joining up care for people, places and populations (February 2022) said "Basic shared

78 NHS Digital, Summary Care Records (SCR)
79 PQ. 259275, Autism and Learning Disability, 11 June 2019
80 NHS Digital, 'Viewing Summary Care Records (SCR)' (last accessed 5 May 2022); Summary Care Records (SCR) (last accessed 5 May 2022).
81 PQ. 115038, NHS: Digital Technology, 1 December 2017
82 NHS England, Joining up health and care data
83 NHS Transformation Directorate (nhsx.nhs.uk), Information Governance Framework: Shared Care Records, February 2022

care records are now in place in all but one ICS", and that everyone should have a shared care record by 2024:

> We will aim to have shared care records for all citizens by 2024 that provide a single, functional health and care record which citizens, caregivers and care teams can all safely access.[84]

[84] Gov.uk, Health and social care integration: joining up care for people, places and populations, 11 February 2022

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 then National Data Guardian for health and care, Dame Fiona Caldicott, in 2016. The Review of Data Security, Consent and Opt-Outs (PDF) 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 for 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.[85]

4.2 Response to the 2017 'WannaCry' cyber-attack

On 12 May 2017, a global ransomware cyber-attack, known as WannaCry, attacked a range of companies and sectors, including the NHS. A National Audit Office investigation found the 2017 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.[86]

It was estimated that the WannaCry cyber-attack cost the NHS £92 million. This figure does not include other impacted organisations.[87] The NHS investigation found that none of the 80 NHS Trusts affected had applied an advised Microsoft patch update.[88]

The Public Accounts Committee highlighted the ongoing threat that cyber-attacks 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.[89]

4.3 Government response on cyber security

In July 2017, the Government published its response to the NDG's Review of Data Security, Consent and Opt-Outs and the CQC's Review 'Safe Data, Safe

85 NDG, Review of Data Security, Consent and Opt-Outs, (PDF) June 2016
86 National Audit Office, Investigation: WannaCry cyber-attack and the NHS (PDF) 25 April 2018, p4.
87 DHSC, Securing cyber resilience in health and care: progress update October 2018 (PDF), October 2018, p14.
88 NHS Improvement, Lessons learned review of the WannaCry Ransomware Cyber Attack (PDF) February 2018, p8.
89 Committee of Public Accounts, Cyber-attack on the NHS, (PDF) 28 March 2018, HC 787 2017-19, para 19.

Care. The report, Your Data: Better Security, Better Choice, Better Care (PDF), also set out learning from the WannaCry attack.

The Government accepted the recommendations of the NDG 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.

In addition to these requirements, from May 2018, under the Data Protection Act 2018 and GDPR, NHS organisations are required to 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.[90]

In February 2018, the Government published Securing cyber resilience in health and care: progress update. The Department made a further announcement of new NHS cyber security improvements in April 2018.[91]

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 said the NHS was putting in place "robust measures" to protect against cyber-attacks, and:

> 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. (...).
>
> 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

90 Information Commissioner's Office, 'Personal data breaches'

91 DHSC, 'Plans to strengthen NHS cyber security announced', 28 April 2018

> healthcare providers) to put appropriate security measures in place and to report significant incidents that occur.[92]

Government progress on NHS cyber resilience was further set out in a report of October 2018.[93] One recommendation from the NHS CIO's WannaCry report (PDF, section 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" had met this standard, compared to 19% in February 2018.[94]

In 2019, the Department said it was continuing to support NHS organisations to upgrade their existing Windows systems to reduce potential vulnerabilities,[95] 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.[96]

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.[97] In July 2019, 0.16% of NHS Machines were still using Windows XP.[98]

92 PQ, 169018, NHS: Cybercrime, 3 September 2018
93 DHSC, 'Securing cyber resilience in health and care', October 2018
94 NHS Digital, 'How we're improving cyber security', 8 October 2019.
95 PQ, 252873, NHS: Cybercrime, 20 May 2019
96 PQ, 254786, NHS Cybercrime, 15 May 2019
97 Committee of Public Accounts, Cyber-attack on the NHS, (PDF) 28 March 2018, HC 787 2017-19, paras 5-7.
98 PQ 277855, NHS: Computer Software,16 July 2019

5 Patient data, Artificial Intelligence (AI) and Apps

5.1 Background

In October 2018, the Department of Health and Social Care, published The future of healthcare: our vision for digital, data and technology in health and care. This set out plans for "robust standards" to ensure "every part of the NHS can use the best technology to improve patient safety, reduce delays, and speed up appointments." The then-Health and Social Care Secretary, Matt Hancock, set out the following ambition:

> 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.[99]

The Government also published A guide to good practice for digital and data-driven health technologies in September 2018. This guidance, which has been subsequently updated, contains a set of principles setting out what the Government expect from suppliers and users of data-driven technologies.

NHSX was established in February 2019, to deliver the Health Secretary's 'Tech Vision' and lead digital policy transformation by bringing together expertise in the DHSC, NHS England and NHS Improvement.

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 said NHS organisations should not enter into agreements that grant one organisation exclusive right of access to raw NHS data, either patient or operational.

In September 2019, the Government said it was developing a set of tools to help technology sellers comply with principle 7 of the code of conduct, which said they should "show what type of algorithm is being developed or deployed, the ethical examination of how the data is used, how its

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

performance will be validated and how it will be integrated into health and care provision."

In November 2021 the Government announced that NHS Digital and NHSX would merge to form part of a new Transformation Directorate within NHS England. The NHS England Transformation Directorate will lead the digital transformation agenda for the NHS and social care at national and Integrated Care System level in England.[100]

This announcement followed an independent review by Laura Wade-Gery, which considered how to ensure a coherent approach to digital transformation in the NHS national bodies. Recommendation 3 of the review was to "commit to building patient and citizen trust and acceptance in the use of health data to improve outcomes. Provide more efficient access to data for analytics that ensures privacy and can be used to improve care delivery."[101]

The Government's white paper Health and social care integration: joining up care for people, places and populations (February 2022) said digital tools "will empower people to look after their health and take greater control of their own care, offering flexibility and support – through the NHS App and NHS.UK, remote monitoring and digital health apps." [102]

In June 2022 the Government published a strategy, Data saves lives, setting out the Secretary of State's vision for how patient data should be used "to bring benefits to all parts of health and social care". The strategy also intends to demonstrate that the health and care system is a trustworthy data custodian. The strategy says it will do this in five ways:

1. Keep data safe and secure.
2. Be open about how data is used.
3. Ensure fair terms from data partnerships.
4. Give the public a bigger say in how data is used.
5. Improve the public's access to their own data.[103]

5.2 Artificial Intelligence in healthcare

There are various applications of Artificial Intelligence (AI) in healthcare, such as helping clinicians to make decisions, monitoring patient health, and

100 Gov.uk, Major reforms to NHS workforce planning and tech agenda, November 2021
101 Gov.uk, Putting data, digital and tech at the heart of transforming the NHS, November 2021
102 Gov.uk, Health and social care integration: joining up care for people, places and populations, 11 February 2022
103 Gov.uk, Data saves lives: reshaping health and social care with data, June 2022

automating routine administrative tasks. A briefing from the Parliamentary Office of Science and Technology (POSTnote, 18 January 2021) gives an overview of these uses, and summarises challenges in the adoption of AI in healthcare, including those relating to privacy, data-sharing, trust, and accountability. It also outlines some of the regulations relevant to AI, and how these may change.

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, she expressed a desire for a review in relation to how the public are informed about their rights in relation to consent and use of anonymised data.[104] She said:

> 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.[105]

In September 2019, there was a Westminster Hall debate on the involvement of patients in the use of artificial intelligence in healthcare.[106] The Commons Library prepared a briefing ahead of this debate (CDP-2019-203, 30 August 2019).

On the 13 September 2019 a BMJ editorial said:

> ...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.[107]

The June 2022 strategy, Data saves lives, says:

> The NHS AI Lab is supporting the advancement of a robust regulatory framework for AI in health and care that supports innovation, and gives patients and clinicians confidence that AI products are safe and effective.[108]

5.3 The NHS App and the NHS Covid Pass

The NHS App was launched on 31 December 2018. The NHS Long Term Plan (January 2019) included a commitment to extend the NHS App to everyone as

104 House of Lords Committee on Artificial Intelligence: Oral Evidence, 21 November 2017, pp17-18.
105 As above, p5.
106 HC Deb, Artificial Intelligence in Healthcare, vol 664, cc 154-175WH, 5 September 2019
107 'New AI laboratory for the NHS', British Medical Journal, 13 September 2019
108 Gov.uk, Data saves lives: reshaping health and social care with data, June 2022

a new digital 'front door' to services, and to give people "secure digital access to their own medical records".[109]

To mark 3 years since the introduction of the NHS App, NHS Digital said, as of 31 December 2021, it has over 22 million users and is one of the UK's most downloaded apps (with over 18 million registrations since the NHS COVID Pass was added on 17 May 2021).[110]

In a speech on digital transformation in February 2022, the Secretary of State for Health and Social Care said he wanted 75% of all adults in England to have the NHS App by March 2024. He also set out how he wanted the App to develop:

> When I think about what the app will look like in the future, I see a platform where you can directly communicate with your health provider, where you can see all your test results and documents in one place, and where you can get personalised advice to manage your own health.[111]

The June 2022 strategy, Data saves lives, reiterated the commitment to having 75% of the adult population registered to use the NHS App and NHS website by March 2024. It also committed to:

> improve access to GP records in the NHS App by giving patients access to their latest health information (November 2022), and provide patients with the ability to digitally request historic coded information including diagnosis, blood test results and immunisations – by December 2023.[112]

The NHS App and Covid Pass service have been developed and managed by NHS Digital and NHSX (which are now part of the NHS England Digital Transformation Directorate).

Online access to Covid-19 vaccination status

The NHS website explains individuals can access a digital version of their Covid-19 vaccination status in two ways, either by using the NHS App or the NHS COVID Pass service.[113]

The Department of Health and Social Care webpage on Demonstrating your COVID-19 vaccination status (last updated 21 June 2021) contains the following information about the data displayed on the NHS App/pass service which relates to a person's Covid-19 status:

> All the information displayed is derived from the National Immunisation Management System (NIMS) database operated by NHS England. The NHS COVID Pass service does not capture any new information. All it does is enable

109 NHS Long Term Plan (2019), Digital Transformation

110 NHS Digital, NHS App turns three with 22 million users, 31 December 2021

111 Speech by Health and Social Care Secretary Sajid Javid at the HSJ Digital Transformation Summit, 24 February 2022

112 Gov.uk, Data saves lives: reshaping health and social care with data, June 2022

113 For people unable to access digital services, the NHS website notes they can request an NHS Covid Pass letter to be sent by post.

> secure access to your immunisation records within NIMS and use a small subset of that information (NHS number, name and COVID-19 vaccination history) to enable the creation of a 2D barcode that can later be shown when travelling abroad. The service has been developed in strict compliance with GDPR and privacy regulations.

The Privacy Notice for the NHS COVID pass which sets out the personal data collected and how it is used, can be accessed via this webpage: NHS COVID Pass - NHS (nhsx.nhs.uk).

The House of Commons Library is a research and information service based in the UK Parliament. Our impartial analysis, statistical research and resources help MPs and their staff scrutinise legislation, develop policy, and support constituents.

Our published material is available to everyone on commonslibrary.parliament.uk.

Get our latest research delivered straight to your inbox. Subscribe at commonslibrary.parliament.uk/subscribe or scan the code below:

commonslibrary.parliament.uk

@commonslibrary