HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 07103, 25 May 2018

Patient health records and confidentiality

By
Elizabeth Parkin

Inside:

Contents

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 making all patient and care records digital, real-time and interoperable by 2020.

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 programme.

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

Contributing authors Alex Bate: Section 1 & 1.1

1. Accessing and sharing patient health records

In 2010, the Department of Health produced *Guidance for Access to Health Records Requests*. This covered legislative basis for patients' access to their health records:

> **The Data Protection Act (DPA) 1998** – governs rights for living individuals to access their own records. The right can also be exercised by an authorised representative on the individual's behalf.
>
> **The Access to Health Records Act 1990** – governs rights of access to deceased patient health records by specified persons.
>
> **The Medical Reports Act 1988** – governs the right for individuals to have access to reports, relating to themselves, provided by medical practitioners for employment or insurance purposes[1]

As of 25 May 2018, access to patient health records is also governed by the EU General Data Protection Regulation (GDPR), enacted by the *Data Protection Act 2018*. The new data protection legislation will also repeal the 1998 DPA. No new Departmental guidance on access to health records has yet been published.

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.

Under the 1998 DPA, an individual was required to request access to their health record in writing, although the 2010 guidance did set out a view that requests could be made verbally where a patient was unable to submit a written request. Under new data protection legislation there are no requirements for a patient to request their records in any specific way. Records must be provided in the same form that they were requested (electronic, hard copy, verbal etc.), where it is practicable to do so.

The Information Governance Alliance (IGA) advises medical data controllers that regardless of whether the request is made verbally or in writing, they are required to check that the requestor is who they say they are.[2]

GDPR also reduces that amount of time within which requested medical records must be provided from 40 days to one month. However, as set out in the 2010 guidance, the Government has made a commitment that health

---

1 Department of Health, *Guidance for Access to Health Records Requests*, February 2010, page 8.

2 Information Governance Alliance, *The EU General Data Protection Regulation: The Key Points for GPs*, March 2018

record requests should normally be handled within 21 days, despite the longer legal time limit.[3]

Hospital records are kept for a minimum of eight years after treatment and GP records for a minimum of 10 years after a patient's death. 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'. 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. The 1988 Act allows GPs to charge reasonable fees for such reports.

A PQ answered in July 2018 explains the change:

> 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 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.[4]

---

3 Department of Health, Guidance for Access to Health Records Requests, February 2010, page 10

4 PQ 162134 [on Medical Records], 12 July 2018

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.[5]

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.[6]

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 to have capacity to give or withhold their consent to the release of information. In Scotland, children aged 12 and over are presumed to have capacity to consent, unless it is otherwise shown that they do not.

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.

---

5 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*.

6 Section 7(4), the *Data Protection Act 1998* and the *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*.

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.[7]

There may also be instances where a relative may be provided access to patient information (see section 2.5).

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 (i.e. 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 a patient requested confidentiality whilst they were alive. No information can be revealed if the patient requested non-disclosure.

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.

For further information on patient confidentiality relating to deceased patients, see section 2.6.

[7] BMA, Confidentiality and disclosure of health information tool kit

2. Sharing confidential patient information

The NHS Constitution 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.[8]

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. [9]

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.

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.[10]

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. Information used in this way must be anonymised and untraceable to individuals before it is released for

---

8 NHS England, NHS Constitution, page 8

9 NHS England, NHS Constitution, page 8

10 BMA, Health and Social Care (Safety and Quality) Bill, House of Lords, Committee stage, 13 March 2015

this purpose. NHS Digital is responsible for ensuring that data is suitable for being used in this way.

2.1 NHS Digital guidance on confidentiality

NHS Digital (formerly the Health and Social Care Information Centre – HSCIC) has a major role in implementing these recommendations. The *Health and Social Care Act 2012* contained a provision that NHS Digital has a statutory duty to produce a Code of Practice for handling confidential information covering "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".

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 Caldicott principles 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[11]

The review recommended that senior individuals are appointed to be responsible for following confidentiality procedures, known as 'Caldicott Guardians'.

2.2 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 NDG's terms of reference set out the three main principles that guide the role:

- encouraging clinicians and other members of care teams to share information to enable joined-up care, better diagnosis and treatment

[11] The guide is supported by a references document which provides more detailed information for organisations and examples of good practice.

- 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.[12]

The 2017 Conservative General Election manifesto set out a commitment to "put the National Data Guardian on a statutory footing to ensure data security standards are properly enforced."[13] This is currently being taken forward through a Private Member's Bill, the *Health and Social Care (National Data Guardian) Bill 2017-19*, sponsored by Peter Bone MP. The Bill will have its Committee Stage on 6 June 2018.

Caldicott principles

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

The 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

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

12 The National Data Guardian's Panel: Terms of Reference, last accessed 25 May 2018

13 Conservative and Unionist Party, Forward, Together: Our Plan for a Stronger Britain and Prosperous Future, May 2017, p80

> 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).

2.3 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.

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). 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.

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 will consult with the NDG on their removal.

Although the opt-out tool was launched on 25 May 2018, health and care organisations have until March 2020 to uphold patient choices.

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

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.[14] Following the review, the then Life Sciences Minister George Freeman confirmed in July 2016 that Care.data was to be closed.[15]

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.

2.4 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.

Additionally, some statues 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.[16] 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.

---

14 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)

15 HCWS62, 6 July 2016

16 BMA, Confidentiality and disclosure of health information tool kit – Card 9: Legal and statutory disclosures

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.[17]

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. 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. 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.[18] 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.[19]

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.

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

> 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 MOU to the Health and Social Care Committee 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.[20]

The amendment was withdrawn. A new MoU is expected to be shared with the Health and Social Care Committee shortly.

---

17 HSCIC, A guide to confidentiality in health and social care, September 2013, page 21

18 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

19 Rt Hon Caroline Nokes MP, Minister of State for Immigration, Home Office, and Lord O'Shaughnessy, Department for Health and Social Care, Letter regarding letter from the Chair to NHS Digital on the Memorandum of Understanding with the Home Office, 23 February 2018

20 HC Deb 9 May 2018, cc756-758

2.5 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.[21]

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. [22]

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:

> Health and care professionals 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.[23]

2.6 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*.[24] 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.[25]

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).

---

21 BMA, Confidentiality and disclosure of health information tool kit – Card 10: Public interest

22 HSCIC, A guide to confidentiality in health and social care, September 2013, page 20

23 HSCIC, A guide to confidentiality in health and social care: references, page 25

24 BMA, Access to Health Records: Guidance for Health Professionals in the United Kingdom, August 2014

25 Department of Health, Guidance for Access to Health Records Requests, February 2010, page 13

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.

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.
>
> 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.[26]

2.7 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.[27]

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.[28]

---

26 General Medical Council, Ethical Guidance for Doctors: Managing and Protecting Personal Information, last accessed 25 May 2018

27 BMA, Confidentiality and disclosure of health information tool kit – Card 7: Adults who lack capacity

28 Code of Practice: Mental Health Act 1983, Chapter 20

3. Electronic health records

3.1 NHS 'paper-free' by 2020

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.[29]

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.[30]

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 comprehensive access – with the ability for individuals to add to their own records – by 2018.[31]
>
> […]

---

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

30 NHS England, Five Year Forward View, October 2014

31 National Information Board, Personal Health and Care 2020, November 2014, page 21

> 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.[32]

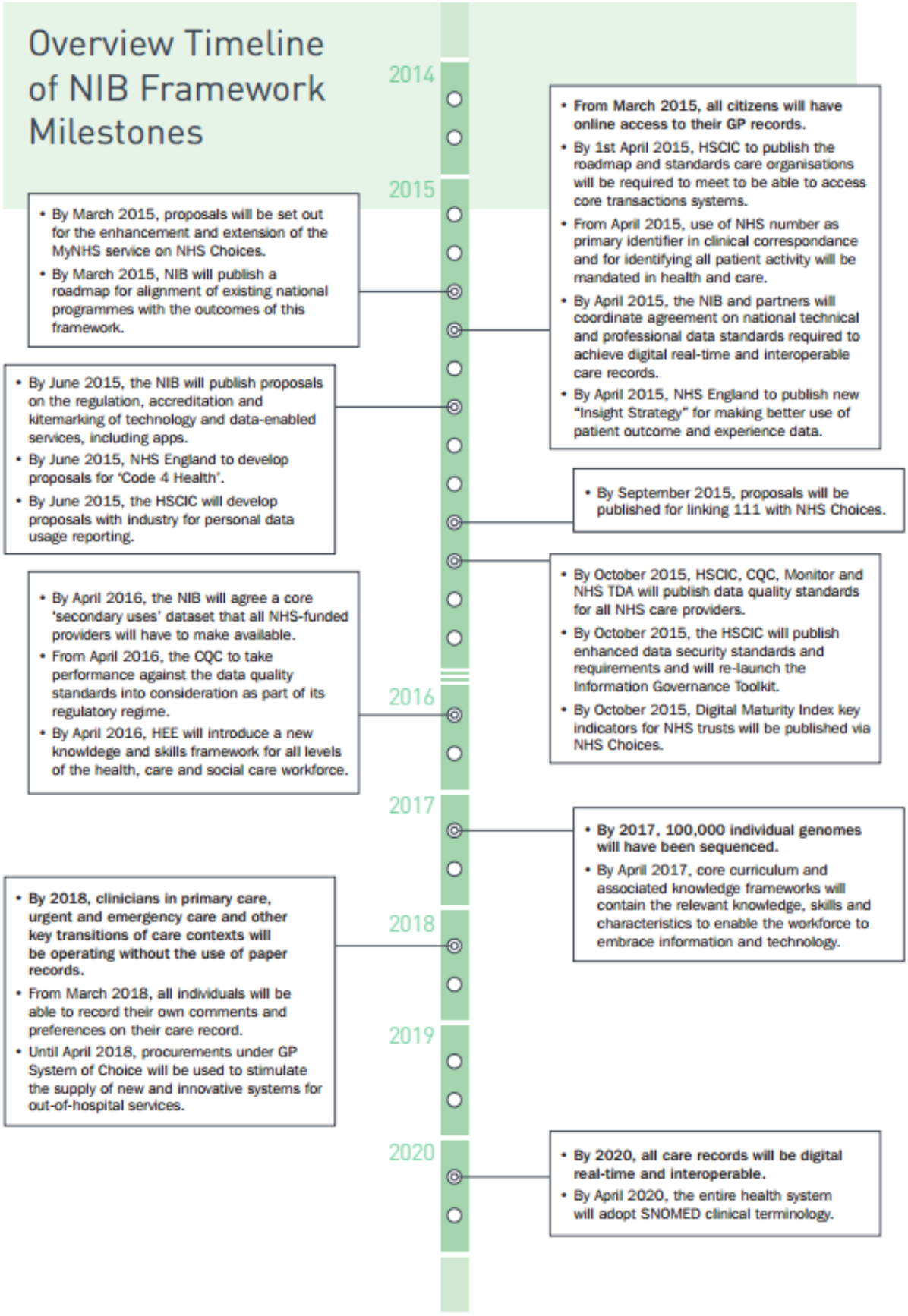
The framework also stated that in April 2016 the Health and Social Care Information Centre (now NHS Digital) would consult on ways of supporting carers to access digital records.[33]

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.[34]

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

The diagram on the following page shows a timeline of the National Information Board's key milestones[35]:

32 National Information Board, Personal Health and Care 2020, November 2014, page 29
33 National Information Board, Personal Health and Care 2020, November 2014, page 31
34 NHS England, Local Digital Roadmaps
35 National Information Board, Personal Health and Care 2020, November 2014, page 58


Overview Timeline of NIB Framework Milestones
2014
2015
2016
2017
2018
2019
2020
From March 2015, all citizens will have online access to their GP records.
By 1st April 2015, HSCIC to publish the roadmap and standards care organisations will be required to meet to be able to access core transactions systems.
From April 2015, use of NHS number as primary identifier in clinical correspondance and for identifying all patient activity will be mandated in health and care.
By April 2015, the NIB and partners will coordinate agreement on national technical and professional data standards required to achieve digital real-time and interoperable care records.
By April 2015, NHS England to publish new "Insight Strategy" for making better use of patient outcome and experience data.
By March 2015, proposals will be set out for the enhancement and extension of the MyNHS service on NHS Choices.
By March 2015, NIB will publish a roadmap for alignment of existing national programmes with the outcomes of this framework.
By June 2015, the NIB will publish proposals on the regulation, accreditation and kitemarking of technology and data-enabled services, including apps.
By June 2015, NHS England to develop proposals for 'Code 4 Health'.
By June 2015, the HSCIC will develop proposals with industry for personal data usage reporting.
By September 2015, proposals will be published for linking 111 with NHS Choices.
By October 2015, HSCIC, CQC, Monitor and NHS TDA will publish data quality standards for all NHS care providers.
By October 2015, the HSCIC will publish enhanced data security standards and requirements and will re-launch the Information Governance Toolkit.
By October 2015, Digital Maturity Index key indicators for NHS trusts will be published via NHS Choices.
By April 2016, the NIB will agree a core 'secondary uses' dataset that all NHS-funded providers will have to make available.
From April 2016, the CQC to take performance against the data quality standards into consideration as part of its regulatory regime.
By April 2016, HEE will introduce a new knowledge and skills framework for all levels of the health, care and social care workforce.
By 2017, 100,000 individual genomes will have been sequenced.
By April 2017, core curriculum and associated knowledge frameworks will contain the relevant knowledge, skills and characteristics to enable the workforce to embrace information and technology.
By 2018, clinicians in primary care, urgent and emergency care and other key transitions of care contexts will be operating without the use of paper records.
From March 2018, all individuals will be able to record their own comments and preferences on their care record.
Until April 2018, procurements under GP System of Choice will be used to stimulate the supply of new and innovative systems for out-of-hospital services.
By 2020, all care records will be digital real-time and interoperable.
By April 2020, the entire health system will adopt SNOMED clinical terminology.

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. 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)[36]

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 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 Summary Care Record.[37]

As of December 2017, 98% of the population in England have a Summary Care Record. In 2017, SCRs were used around 6.5 million times.[38]

Rollout of SCRs also covers community pharmacies. As of October 2017, 96% of pharmacies in England had read access to SCRs, with 80% having a secure NHS email account to contact GPs regarding patient encounters.[39]

---

36 NHS Digital, Summary Care Records (SCR), last accessed 25 May 2018

37 For the opt-out process, see NHS Choices, Information about different types of health records, last accessed 25 May 2018

38 PQ 115038, 1 December 2017

39 PQ 107291, 19 October 2017

4. NHS data and cyber security

The Secretary of State for Health, Jeremy Hunt, stated in the foreword of the 2017 Government report on data security, that using patient information safely and securely, as well as protecting against data and security threats "underpins our ambition of having a world class health and social care system in the digital age."[40]

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.[41]

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

---

40 Department of Health, Your Data: Better Security, Better Choice, Better Care, July 2017

41 Committee of Public Accounts, *Cyber-attack on the NHS*, 28 March 2018, HC 787 2017-19, para 19

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.[42]

4.2 Government response (2017)

In its 2017 response to the review, the Government accepted the recommendations and standards, 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 standard number 6, noting that serious cyber-attacks should be reported to CareCERT[43] immediately. It also confirmed that harsher sanctions for malicious or intentional data security breaches would be brought in by the new 2018 data protection legislation.

In addition to these requirements, as of 25 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 under the new data protection requirements.

Further NHS cyber security improvements were announced by the Department of Health and Social Care in April 2018:

> A new multi-million pound Microsoft package will ensure NHS systems have the most up-to-date software with the latest security settings.
>
> The deal with Microsoft will ensure all health and care organisations are using the latest Windows 10 software with up-to-date security settings to help prevent cyber attacks.
>
> Since 2017 the government has invested £60 million to address cyber security weaknesses. A further £150 million will be spent over the next 3 years to improve the NHS's resilience against attacks. This will

42 National Data Guardian for health and care, *Review of Data Security, Consent and Opt-Outs*, June 2016

43 NHS Digital's Care Computer Emergency Response Team

include setting up 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
- 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 data security and protection toolkit which requires health and care organisations to meet 10 security standards
- a text messaging alert system to ensure trusts have access to accurate information – even when internet and email services are down[44]

These new measures came partially in response to the WannaCry ransomware attack. At the time of the attack, 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.[45]

---

44 'Plans to strengthen NHS cyber security announced', *Department of Health and Social Care press release*, 28 April 2018

45 Committee of Public Accounts, *Cyber-attack on the NHS*, 28 March 2018, HC 787 2017-19, para 5-7

BRIEFING PAPER
Number 07103, 25 May 2018

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