NDG National Data Guardian
for health and social care

The National Data Guardian for Health and Social Care

Annual report 2019-2020

Published 30 July 2020

Contents

Foreword by Dame Fiona Caldicott

Dame Fiona Caldicott

National Data Guardian for Health and Social Care in England

The COVID-19 emergency has required a programme of massive change across health and social care, and indeed throughout our country. Established procedures that we thought were hardwired into the system have been amended at lightning speed, as staff have rallied to respond to the crisis. I pay tribute to the skill and bravery of all the professionals and those supporting them.

I was pleased to play a part in ensuring temporary adjustments were made to regulations in order to smooth the flow of health and care information across organisational boundaries in the interests of public health. In fact, existing law permits considerable flexibility in a public health emergency, allowing confidential data to be used for some purposes without obtaining people's consent. To its credit the Department of Health and Social Care has been very clear that this use of emergency powers is not open ended. There will be a review before the arrangements end in September 2020 to consider whether they should continue and, if so, for how long.

There have been many examples of rapid action to use data in the public interest, such as NHS Digital providing information to help identify extremely vulnerable citizens very quickly, so that they can be assisted, and NHSX producing guidance for clinicians on appropriate ways to communicate, share information and deliver care rapidly.

Some departures from normal practice have been so beneficial that we may want them to be continued in the long term. For example, the emergency powers allow clinicians to share additional information in a patient's Summary Care Record, beyond the bare minimum, without having to seek the patient's consent again to do that. When we have asked the public about such data sharing to support their own care, we have heard clearly that people want such information to be available wherever they seek care. In my view, that is an entirely sensible approach that should have been happening anyway. If a patient provides information to one hospital department and then attends for treatment in another, they do expect their information to flow across smoothly. Now the emergency has brought a quick and pragmatic solution. I do not believe it would make sense to go back to the old way of doing things.

However, we must not allow the pandemic to become an excuse for permanently abandoning limits on the use of confidential information that are essential for maintaining the public's trust. There is a danger that some people and organisations might seek to take advantage of this situation. However, the rules approved that require careful scrutiny of applications to use confidential information remain important to secure the confidence of patients and those using social care. They are important to maintain public trust.

As we move out of the initial response to the pandemic and into a phase when data will be used in sophisticated and targeted ways to trace disease spread and outbreaks, it is more important than ever that citizens are informed about what is happening with their information. As citizens we all have a stake in the success of this endeavour and the willingness of the public to participate is critical to its effectiveness. Building and maintaining public trust about data usage is an essential element of maximising that participation.

One consequence of the emergency is an advance in public understanding of the role that data may play. For many years I have been commenting with some regret that most people seem to know little about how their health and care data is used by the services that collect it. I wanted them to know more and now, quite suddenly, it seems that the public has come to have more awareness about that. Statistics on disease spread and tragic deaths have become a matter of daily reporting and public discussion. The public knows more about how the health and care system is organised and quite a lot about how data is used. The publicity around the test and trace programme in particular has made people think about this subject. So, as we come out of the pandemic, we will have a more aware public, I believe. We may find that people have stronger feelings about how their data is being used. We will have to engage with them to learn what their views are and to do what is necessary to earn their trust.

In spite of all the changes in how data has been handled during the COVID-19 emergency, it is important to note that there has been no requirement to adapt our enduring values. Data should be used proportionately and transparently in the best interests of individuals and society.

It was my privilege to play a part in crafting those enduring values into the set of principles that came to bear my name. In 1996/7 I was asked to lead a Government review of what were the proper uses of patient-identifiable information. It was a time of widespread concern about how the development of IT systems across the NHS might spread information about patients that had previously remained protected in doctors' local premises. That early work was very difficult, and it was not at all clear that we would obtain agreement from the broad range of interested parties that were involved. Nevertheless, we were able, through that group of some 50 people or so, to develop principles that have stood the test of time. People have found them useful.

We set out six Caldicott Principles in 1997. The Information Governance Review that I led for the Government in 2013 added a seventh to draw attention to the fact that the duty to share information appropriately may be just as important as the need to protect it from inappropriate disclosure. Now my panel and I are considering the introduction of an eighth Caldicott Principle to remind staff across health and social care that there should be “no surprises” for patients and service users when they discover how their data has been used and shared. This eighth principle will underline the importance of considering and informing people's expectations to promote understanding and acceptance about the use of data. We want to help the public to obtain the knowledge that they need in order to make choices about their health and wellbeing.

If it had not been for the COVID-19 epidemic, we would already have launched a full public consultation on the eighth principle, accompanied by workshops for members of the public to have their say. That started later than planned and has been extended over a longer period to allow colleagues busy with COVID-19 activities more time to respond. This consultation will also canvass opinion about minor changes to the wording of the existing Caldicott Principles to ensure they remain up-to-date and as useful as possible. I will seek views about a proposal to use my statutory powers to issue guidance about organisations appointing Caldicott Guardians to uphold the Caldicott Principles. It was with a degree of amazement that I discovered recently that there are now more than 18,000 Caldicott Guardians in England. They deserve support.

A Caldicott Guardian is a senior person within a health or social care organisation who makes sure that the personal information about those who use its services is used legally, ethically, and appropriately, and that confidentiality is maintained. They perform a valuable role providing the conscience of their organisations, but they would benefit from clear guidance about how their role dovetails with other roles in data management.

I am in post as National Data Guardian until March 2021 and I expect to step down at that point. The discussions about what data sharing should look like after the COVID-19 crisis will start to take place before then and I will be a part of that. No doubt they will continue after I have left.

I was a psychiatrist whose clinical practice centred on confidential conversations with people. However, my expertise in information governance when I started the review of patient-identifiable information in 1996 was not extensive, and I have learned a lot about the subject since. Most importantly I have come to understand that, as circumstances change, it is the enduring values that matter most. They are not straightforward to uphold. Words such as respect, choice, dialogue, consent, and trustworthiness are easy to use, but living by them is hard. That is what we must continue to endeavour to do. Those needing health and care services can then have faith that their precious information is safeguarded and used for their benefit, and when they choose, for the wellbeing of others as well.

I would like to close by saying how much I appreciate the support of colleagues that I have had in pursuing my work. Being the National Data Guardian has never been a one-woman activity. I have benefitted hugely from the advice of my panel of experts, who have been extremely generous with their time and wise in their judgements. I have also had great support from the various teams of officials with whom I have worked over the years.

With warm thanks and best wishes to you all.

Dame Fiona Caldicott

MA FRCP FRCPsych

National Data Guardian for Health and
Social Care in England

1 Introduction and background

This report gives an account of work done by the National Data Guardian for Health and Social Care in the first year since her position gained statutory authority on 1st April 2019.

Preparation began in February and March 2019 when she initiated a formal, public consultation about what the NDG's priorities should be. She invited comments from patients, service users and other organisations and groups that have a role to play in the use of health and care data. Her resulting consultation response, published in July 2019[1], outlined what were to be the NDG's three key priorities, each broken down into a number of work areas. The three priorities were:

- Supporting public knowledge and understanding.
- Encouraging information sharing for individual care.
- Safeguarding a confidential health and care system.

This report is structured to examine each of those priorities in turn, looking at what has been done in the first year to meet the desired objectives and fulfil the commitments that underpinned them. It should be stressed that it was never anticipated that this work would be completed in a single year. The priorities remain in place and further progress is anticipated in 2020-21 and beyond. It should also be noted that the three priorities were not intended to be ranked in order of importance: they are of equal significance.

During the period covered by this report the NDG has been supported by a small team of officials and a panel of independent advisers, who are listed in Appendix A. The panel's terms of reference and the minutes of its deliberations are available on the NDG's webpages[2]

Background

Legislation to enhance the authority of the National Data Guardian passed unamended through the House of Commons and House of Lords thanks to cross-party support. The Health and Social Care (National Data Guardian) Act 2018[3] received Royal Assent on 20th December 2018. Matt Hancock, the Secretary of State for Health and Social Care, signed an order to provide for the commencement of the provisions of the Act from 1st April 2019 and confirmed that Dame Fiona Caldicott would be the first holder of the office for a term of 18 months.

The Act gave the NDG the ability to issue guidance about the processing of health and adult social care data in England. Public bodies, such as hospitals, general practices, care homes, planners, and commissioners of services, have to take note of guidance that is relevant to them. So do organisations such as private companies or charities which are delivering services for the NHS or publicly funded adult social care.

Although the Act provided the NDG with new powers, they were a continuation of the work that Dame Fiona had been doing since November 2014 when the previous Secretary of State appointed her as the (non-statutory) NDG, pending Parliamentary approval of formal powers.

The foundation for her work in this field was the Information Governance Review[4] that she carried out for the Department of Health, which reported in April 2013. This became known as the Caldicott2 Report to distinguish it from an earlier report that

---

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/815950/1037_-_NDG_consultation_response_10.07.19_FINAL_TO_PUBLISH.pdf
[2] https://www.gov.uk/government/publications/national-data-guardian-panel-meeting-minutes-2019
https://www.gov.uk/government/publications/national-data-guardian-panel-meeting-minutes-2020
[3] http://www.legislation.gov.uk/ukpga/2018/31/contents/enacted/data.htm
[4] https://www.gov.uk/government/publications/the-information-governance-review

she delivered to the department in 1997[5]. The Government accepted all the 26 recommendations in the Caldicott2 Report and the Secretary of State asked Dame Fiona to set up a new independent panel to monitor progress and provide independent advice and challenge to the whole health and care system. The Independent Information Governance Oversight Panel (IIGOP) produced a progress report in January 2015[6].

Dame Fiona published a subsequent account in December 2017 describing her work as NDG during 2015-17 and setting eight priorities for 2018[7]. A further report in August 2019[8] gave an account of activity under each of the priority headings and completed the record of what was achieved before the statutory powers came into operation.

The NDG is required to produce an annual report including information about advice given, guidance published in the previous financial year, and the priorities for the forthcoming year. Expenditure is reported through the DHSC Annual Report and Accounts. It is these responsibilities that are being discharged in this report.

---

[5] https://webarchive.nationalarchives.gov.uk/20130124064947/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdfhttps://webarchive.nationalarchives.gov.uk/20130124064947/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf

[6] https://www.gov.uk/government/publications/iigop-annual-report-2014

[7] https://www.gov.uk/government/publications/national-data-guardian-2017-report

[8] https://www.gov.uk/government/publications/national-data-guardian-2018-19-report

2 Progress against the National Data Guardian's priorities

2.1 Priority: Supporting public knowledge and understanding

Summary of progress

Patient access to their health and care records

What we said we would do:

"We will work with the relevant bodies to explore the barriers to improving patient access to their records and to information about how data about them has been used."

What we did:

- We commissioned opinion research to test the public's appetite for greater access to records. Two-thirds wanted access to a fuller online GP record, and more than half would want to know if data about them was used by planners or researchers.
- We called for more work to be done on a viewing tool for citizens to see how their data had been used for purposes other than their individual care.
- We ran an online survey of healthcare professionals which found strong support for giving people easier access to their own records. Most thought this may help improve data quality and drive down barriers to wider information sharing.

Transparency and public engagement

What we said we would do:

"We will continue to champion the NDG's long-standing principle that those using and sharing data must be transparent and that they must engage with the public and patients so that the case for data sharing is made."

What we did:

- We gave advice during the COVID-19 pandemic on emergency arrangements to facilitate the sharing of data to ensure it would be transparent, well explained, with appropriate safeguards and time limited.
- We gave advice to health and care organisations to encourage effective engagement with the public; and we praised good practice in several examples of transparency and effective engagement by a number of other organisations.
- We gave advice to NHSX[9] that "type 1 objections"[10] should remain in place until there had been effective engagement with citizens and GPs. NHSX agreed.

---

[9] NHSX is a joint unit, formed in 2019, which brings together teams from the Department of Health and Social Care, NHS England and NHS Improvement to drive the digital transformation of care. It is responsible for setting national policy on NHS data and technology.

[10] The type 1 objections were introduced in September 2013 to allow patients to stop information about them leaving their GP practice in an identifiable form for purposes beyond their direct or individual care. In 2017 the Government said the policy would be subject to review in 2020.

Benefits of health and care data

What we said we would do:

“We will examine what additional public engagement would be most useful on the subject of the benefits from the use of health and care data. We will continue to support the work to develop a framework to realise the benefits for patients and the NHS where health and care data is being used to underpin innovation.”

What we did:

- We worked with Understanding Patient Data and the Sciencewise programme to develop a project to explore questions about public benefit from the use of health and social care data in a series of public dialogue workshops.
- Subject to compliance with COVID-19 safety restrictions, these are due to take place at four locations across England in autumn 2020.
- The workshops will ask: if the sharing of health and care data for planning or research is justified on the grounds of public benefit, how is that defined and measured?

Priority progress in-depth

Patient access to their health and care records

What we said we would do:

“We will work with the relevant bodies to explore the barriers to improving patient access to their records and to information about how data about them has been used.”

The Information Governance Review[11] that Dame Fiona chaired in 2012-13 made 26 recommendations, all of which were accepted by the Government.[12] Recommendation 1 said:

“People must have the fullest possible access to all the electronic care records about them, across the whole health and social care system, without charge.

“An audit trail that details anyone and everyone who has accessed a patient’s record should be made available in a suitable form to patients via their personal health and social care records. The Department of Health and NHS Commissioning Board[13] should drive a clear plan for implementation to ensure this happens as soon as possible.”

Although some improvements were made in subsequent years, notably by GPs providing patients with online access to some of their medical records, progress in implementing this recommendation was slow.

As NDG, Dame Fiona returned to this theme in 2016 in her Review of Data Security, Consent and Opt-outs.[14] Its recommendation 18 said:

“The Health and Social Care Information Centre (HSCIC)[15] should develop a tool to help people understand how sharing their data has benefited other people. This tool should show when personal confidential data collected by HSCIC has been used and for what purposes.”

After public consultation, the Government in July 2017 accepted all the recommendations of the Review[16]. In relation to recommendation 18 its response said:

“NHS Digital will update its data dissemination register to be more explicit about the purposes that the data they disclose has been used for, and will include the benefit described by the data applicant in their application. By December 2018, people will be able to access a digital service to help them understand who has accessed their summary care record. By March 2020, it will also enable people to use online services to see how their data collected by NHS Digital has been used for purposes other than their direct care.”

This sounded promising. During the consultation in 2019 on the priorities that should guide the NDG when the office was put on a statutory footing, respondents supported the pursuit of greater transparency. Many wanted to see tailored information showing how data about them has been used for reasons other than their own individual care, for example how it has been used to improve health, care and services through research and planning. Respondents anticipated positive results from this proposal, the most frequently mentioned benefit being a reduction of mistrust in data sharing.

Polling evidence about support for greater record access

As a starting point, the NDG commissioned opinion research to test the public’s appetite for greater access to records. This was conducted by research company

---

[11] https://www.gov.uk/government/publications/the-information-governance-review

[12] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF.

[13] The NHS Commissioning Board came to be known as NHS England.

[14] https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

[15] The HSCIC is now known as NHS Digital.

[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/627493/Your_data_better_security_better_choice_better_care_government_response.pdf

Kantar in April 2019 as part of an omnibus poll of 2,221 English adults aged 16+. Results were weighted.

It found strong support for access to a fuller online GP record than is usually available currently. Nearly two thirds of those polled (65%) said it was important to them to have full access to their GP patient record online, including detailed information about their health, such as diagnoses, illnesses, referral letters, test results, operations etc. Among those who already had access to a basic version of their GP record, there was a greater proportion saying that full access is important to them (78%).

The poll also asked people what they would want to use the access for, asking them to rank a list of possible functions from most to least important. The function rated as most important by the largest proportion of people was the ability to check whether the record was accurate; 23% of respondents chose this. Another 18% of respondents ranked managing their own health as the most important function, 15% said curiosity/interest, 14% said helping to prepare for appointments or check details afterwards, and 12% said it was most important to check who has looked at their record.

The poll also asked about some purposes connected with wider use of individuals' data, such as giving permission for their information to be used for a medical research project and seeing whether their information has been used in research. These were nominated as the most important by only 4-5% of people, but they were ranked in the top four functions by around a third.

The NDG commissioned further polling in February 2020 to test public knowledge of how health and care data is used and ask people what they would want to know and what choices they have. This was again conducted by research company Kantar as part of an omnibus poll of 2,222 English adults aged 16+. Results were weighted. More than half (55%) said they would want to find out when a project using NHS patient data had used information about them; and a similar proportion (52%) would register with an online service where they could find out whether any projects have used data.

Data use viewing tool for citizens

The NDG learned in autumn 2019 of a decision made by the National Data Opt-out Programme (NDOP) board to agree that work by them on creating an online service for citizens, to see how their data collected by NHS Digital had been used for purposes other than their individual care, should be discontinued. The reasons outlined were that research had shown that there was very low demand for such a service; that a more viable approach would be to improve the existing sources of information for individuals wanting to know how their data had been used; and that the programme itself was closing earlier than anticipated so that it was not possible for the work to be continued in that forum.

Dame Fiona expressed her disappointment to NHSX[17] in its capacity as the body that had led the NDOP board. She explained that she and her panel advisors felt that there was insufficient evidence to conclude that there was little demand for such a service. The low level of awareness about the uses of health and care data and the importance of ensuring 'no surprises' for the public are strong reasons for providing more information to the public. As the experience of the National Data Opt-Out launch has shown, when time and care is taken to provide clear, accessible, transparent information, public trust may be strengthened.

The NDG reiterated her wish to see more work on options for enabling members of the public to see how their own data has been used for purposes other than their individual care. Meanwhile, Dame Fiona also welcomed that NHS Digital was considering how to improve information on its website about how it uses data. She agreed that information such as that

---

[17] NHSX is a joint unit, formed in 2019, which brings together teams from the Department of Health and Social Care, NHS England and NHS Improvement to drive the digital transformation of care. It is responsible for setting national policy on NHS data and technology.

provided in the data release register[18] could be much more user-friendly.

Although progress on the individual data tool was not as good as had been hoped, the NDG and her panel pushed forward on other fronts to respond to the public's appetite for greater access to records, as had been demonstrated by the polling results.

Maturity model for patient-facing digital services

Professor Martin Severs, a member of the NDG's Panel, developed a theoretical model to demonstrate how patient-facing digital services that allow people to view their own records might advance through various levels of sophistication. His schema categorised five different levels according to how much or how little a service would offer to patients. As a minimum, the digital service would enable a patient or service user to access and copy information about their own individual care. As a maximum, an individual would be in control of their own personal care record, which could include all the data about them generated by health and care services as well as data they generated themselves, including their own readings and wellbeing data. At this level of sophistication, citizens would be able to use the record for a variety of purposes, including self-care. Third parties wanting to access a person's data for secondary purposes would seek permission via the digital service provider. The patient or service users could consent to such sharing, or not.

The schema could be used to assess the stage which a digital service has reached and how near digital services are to best in class. It is to be shared on the NDG's webpages to gather feedback to improve its usefulness.

Exploring barriers to information sharing for individual care

Further support for citizens gaining more access to their records came from work led by Dr Alan Hassey, another member of the NDG's Panel, to identify the barriers that are impeding effective information sharing among the professionals involved in people's individual care. As part of this work, the NDG commissioned an online survey to help her better understand the perceived barriers. It included a questionnaire that was completed by 65 organisations and individuals engaged in this field. The survey ran from 23rd December 2019 until 2nd February 2020.

Among the propositions presented for consideration were two of particular relevance to record access.

More than two-thirds of respondents agreed or strongly agreed with the statement: "Easier access by patients to their own data may help improve data quality and drive down barriers to wider information sharing." Some respondents entered important caveats. One noted that to talk of an individual's "own" data is not strictly correct: the issue is not about ownership, but access to health and care records *about* the individual. Others observed that people do not have a right to change information in their records unless it is incorrect, and that the content may be complex, sensitive and require expert interpretation. Also access arrangements for shared records need to be coordinated across a health and care community so practice is consistent and sensitive to issues such as third-party information. Other respondents commented on the clinical benefits of giving citizens access to their records. One respondent observed: "When patients are able to access their own data, this enables them to gain a full overview of the care they are receiving, as well as all their test results and other medical information, empowering them to more effectively advocate for the care and support they need. It also allows them check whether their medical record is accurate and up to date, and to share the information in it with whoever they consider appropriate."

A second proposition was that: "There should be a presumption that patients have access to their care records. Where patients have not been given such access, their care professionals should be able to provide clear reasons why not." More than 80% of respondents agreed or strongly agreed with this approach to giving people access, which is in keeping with their

---

[18] https://digital.nhs.uk/services/data-access-request-service-dars/register-of-approved-data-releases

rights under GDPR. However, respondents also highlighted the technical, legal, organisational and workload barriers that will need to be addressed if providing access to health and care records is to become a system-wide reality.

The NDG prepared a report on this exercise including a recommendation to "develop an approach to ensure patients, carers and service users can access important information about their health and care in ways that help them understand the content and context of that information." The NDG will work with other system stakeholders with the aim of ensuring that these recommendations are taken forward.

The NHS App

During 2019-20 the NDG engaged with the team at NHS Digital that was developing the NHS App[19] and its commissioner at NHSX. The NHS App provides a simple and secure way for people to access a range of NHS services on their smartphone or tablet. It enables people to check their symptoms, order repeat prescriptions, book appointments, register their organ donation decision and more. The app is available to everyone in England aged 13 and over. To date, more than 800,000 people have registered to use it, and they have viewed their GP medical records via the app more than 2.5 million times. Individuals can also use the app to set their National Data Opt-out decision, and it has been used over 3,000 times so far to do so.

Members of the NDG's Panel and Steering Group used the NHS App during its beta testing phase and provided feedback to the NHS App programme at NHS Digital. The NDG and her panel have remained in regular contact with the team throughout the app's development and rollout. The potential of the NHS App to help individuals access their medical records was a key issue of discussion.

Since February, the NHS App team has been focused on supporting health and care professionals and individuals through the COVID-19 crisis. It has implemented new, useful features such as the ability to view and change the pharmacy to which a patient's prescription is sent; the ability to send secure messages between practice and patient; expanding online consultation functionality; enabling some users to access health services on behalf of someone they care for, such as a child or elderly relative. The NDG commends the NHS App team for their quick and responsive work.

Transparency and public engagement

What we said we would do:

"We will continue to champion the NDG's long-standing principle that those using and sharing data must be transparent and that they must engage with the public and patients so that the case for data sharing is made."

COVID-19: encouraging transparency about data use

A prime example of the importance of transparency came when the COVID-19 pandemic struck in the spring of 2020. Clearly exceptional steps had to be taken, including activation of emergency arrangements to facilitate the sharing of data.

The COVID-19 response proved just how effective our confidentiality safeguards are, and how quickly laws and clauses supporting the sharing of confidential patient data in a time of crisis can be brought into operation. This included the formal notices published by the Department of Health and Social Care, which required healthcare organisations, GPs, local authorities, and arm's length bodies to share confidential patient information to support efforts against coronavirus. It was clearly stated that these arrangements were limited to COVID-19 purposes, for a time-limited period (initially to 30 September, with scope to extend) and required organisations to keep records of all data processed.

There were many examples of rapid action and problem solving, such as NHS Digital providing information to help identify the

---

[19] http://www.nhs.uk/app (not to be confused with the *NHS COVID-19* app https://covid19.nhs.uk/)

most at-risk citizens very quickly, and NHSX providing guidance to health and care staff on appropriate ways to communicate, share information and deliver care. The NDG gave support by reviewing and endorsing these actions and guidance.

We know from previous dialogue with the public, conducted by the NDG and others, that there is strong support for the use of health and care data where there is a clear public benefit. People are generally altruistic about the use of their data and want it to be used to help others as long as there are appropriate safeguards in place. However, it is important that patients and service users are kept fully informed. Even in times of crisis, protecting trust in confidential health and care matters. The guidance and notices issued to allow data sharing to combat the COVID-19 outbreak contained appropriate safeguards: limiting the purposes for which data can be used, who can use it and the amount of time for this to occur. These were important protections that patients would have been glad to hear about.

It was gratifying that, in the thick of everything, colleagues cited the importance of protecting confidentiality. Practical steps were also taken to ensure that trust was not undermined. For example, the NDG was pleased to support NHSX with the drafting of a template privacy notice, which was sent out to NHS organisations to support them in telling patients and social care service users about what might be different in the handling of their health and care data during the outbreak.

As the pandemic continued, the NDG and her panel continued to monitor the response to COVID-19 and stood ready to support their colleagues across health and care in any way possible.

In March 2020, members of the NDG's Panel joined the Ethics Advisory Board[20] (EAB) set up by NHSX to advise on the development of an NHS COVID-19 contact tracing app. The app had potential to support the management of the pandemic and potentially the lifting of some restrictions. If it was to fulfil this potential it was vital that it worked effectively and that it was clear to individuals who were being asked to download it how their data would be used and what choices they would have. The NDG involvement in advising on the app emphasised the importance of ensuring that the app brought genuine value to the individuals using it and that all uses of data were transparent.

During the pandemic, the NDG encouraged and reminded organisations of the importance of providing clear, accessible information to the public. While the NDG understood that data sharing arrangements sometimes had to be put in place at speed, she also maintained the view that the public should be left with no surprises about how their data was being used.

Transparency at work: examples of good practice in public engagement

This annual report provides an opportunity for the NDG to praise examples of good practice from across the health and care system.

Local Health and Care Record Exemplars

These included useful work in the Local Health and Care Record Exemplar (LHCRE) areas in several parts of England to inform the public about how data flows across organisational boundaries. For example, the OneLondon LHCRE collaborative developed its data sharing model by embarking on extensive engagement with Londoners to shape how information would be used to improve care for individuals, families and communities. The aim was to empower citizens to have their say, and to inform policy and practice in a way that builds legitimacy, trust, and confidence. The multi-stage engagement programme included a particular focus on engaging marginalised and vulnerable communities to understand their views. Social researchers spent time in homeless shelters, interviewing people who do not speak English, working with members of the gypsy and traveller communities, going to places of worship to talk to religious

---

groups, and engaging with members of the LGBTQ+ community.

This culminated in the design and delivery of a London-wide Citizens' Summit - a public deliberation which brought together 100 people (reflective of London's diverse population) to form recommendations as to how Londoners' health and care data should be used. Over two weekends, participants were educated about some of the complex topics related to data access and use, putting them in a good position to deliberate some of these challenges in depth. As such, they were able to reach an informed, considered and civic-minded view. Their recommendations were received by local and national policymakers, politicians and system leaders, and will be used to inform policy for London.[21] The recommendations have been formally published in a report titled: Public deliberation in the use of health and care data.[22]

Connected Health Cities

Another example of good practice in engagement was Connected Health Cities (CHC)[23], a Government-funded programme that ran from 2016 to 2020. It used information and technology to improve health and social care services for people across the north of England. In a bid to hold a sustained and meaningful discussion with its citizens, CHC used a range of complementary methods and approaches, with citizens participating in both core activities and also outreach into communities. The programme used, and contributed to, the successful social media campaign #DataSavesLives – a public engagement campaign to highlight the positive ways that patient data is securely re-used to improve health services. It also partnered previously with the NDG in organising a citizen's jury[24] to explore patients' reasonable expectations about how their data would be used.

When the programme concluded this year, the NDG said: "I commend Connected Health Cities for its commitment to public engagement and its dedication to understanding what patients and the public truly think about the use of their health and care data. Such meaningful engagement is vital if we are to gain people's trust and win their support for the use of their information in initiatives that may see data being used in new and innovative ways."

Understanding Patient Data's 'Foundations of Fairness'

The NDG also praised the public engagement programme, led by Understanding Patient Data (UPD), to explore what the public believes is a fair health data partnership between the NHS and third parties such as researchers, charities, and industry[25]. The work was co-commissioned with NHS England, in partnership with the Ada Lovelace Institute and the Office for Life Sciences (OLS). Their report found "that the public will only support third parties using NHS-held health data when there is benefit to patients across the UK, rather than short-term financial gain for the NHS." Benefits to patients included examples such as improving disease detection or developing new medicines and treatments. The NDG's involvement in this UPD project included participation by Professor James Wilson, a panel member, in an oversight group which advised on the public dialogue.

Encouraging others to engage with the public about data

Health Data Research UK

We provided guidance and support several times during 2019-20 to Health Data Research UK[26], the national institute for data science in health, to assist parts of its Digital Innovation Hub programme. In particular we encouraged it to engage and

---

[21] Further information available at www.onelondon.online, or follow @OneLondon4 on Twitter

[22] https://www.onelondon.online/wp-content/uploads/2020/06/Public-deliberation-in-the-use-of-health-and-care-data.pdf

[23] https://www.chc-impact-report.co.uk/

[24] https://www.gov.uk/government/speeches/talking-with-citizens-about-expectations-for-data-sharing-and-privacy

[25] https://understandingpatientdata.org.uk/news/accountability-transparency-and-public-participation-must-be-established-third-party-use-nhs

[26] HDR UK's team of experts develop and apply cutting-edge data science approaches to clinical, biological, genomic and other multi-dimensional health data to address the most pressing health research challenges facing the public. Further information at www.hdruk.ac.uk

involve practitioners, patients, social care users and the public.

Type 1 objections

The NDG also advised the Department of Health and Social Care that arrangements for the so-called “type 1 objections” should remain in place to allow time for effective engagement with citizens and GPs. The type 1 objections were registered by nearly 1.9 million people who did not want information about them leaving their GP practice in an identifiable form for purposes beyond their direct or individual care[27]. The policy was introduced in September 2013 by the former Secretary of State for Health. The NDG’s Review of Data Security, Consent and Opt-outs in July 2016 recommended a simplified national opt-out that would replace the complex array of pre-existing opt-outs, including the type 1s. This was accepted in the Government’s response published in July 2017, which said that the health and care system would honour the type 1s until 2020 to allow the new national opt-out to be implemented, and for full engagement with primary care professionals and the public. The response committed to consult the NDG before confirming the removal of type 1 opt-outs.

The NDG’s advice to the Department of Health and Social Care this year was that the type 1s should remain in place to allow more time to liaise with GPs and the public about this safeguard. Dame Fiona recommended that any move to remove these arrangements should require another significant programme of work to encompass technical and policy issues as well as full engagement with primary care professionals and the public. NHSX replied in November 2019: “We have taken the decision not to remove type 1 opt-outs until the GPDfPR [GP Data for Planning and Research] is established and the pseudonymised at source solution is in place, alongside a range of other safeguards, to command the trust of patients and the public. We will consult you further before confirming the removal of type 1 opt-outs.”

Benefits of using data

What we said we would do:

> “We will examine what additional public engagement would be most useful on the subject of the benefits from the use of health and care data. We will continue to support the work to develop a framework to realise the benefits for patients and the NHS where health and care data is being used to underpin innovation.”

Exploring perceptions of public benefit

Previous research has shown that the extent of public benefit is the key condition determining people’s acceptance of the use of health and care data for purposes other than their own individual care[28]. During the consultation that the NDG ran about her priorities in 2019 we heard a demand for more clarity on the topic, which would allow decisions about data use to be made more consistently and with confidence.

In response, the NDG worked with Understanding Patient Data and the Sciencewise[29] programme to develop a major project which will see issues around public benefit discussed in a series of public dialogue workshops. These will examine questions including:

- How is the perception of benefits and disbenefits affected by the identity of those who benefit or are disadvantaged?
- What is the scale for measuring any benefit and disbenefit?
- How close should the benefit be to the original purpose of the data collection?

The dialogue is being delivered by public engagement specialists Hopkins Van Mil and will be held at four locations across England: Reading, Stockport, Great Yarmouth, and Plymouth. Subject to

---

[27] As at 10 June 2018 there were 1,888,973 instances of type 1 opt-out codes occurring within GP records, preventing these records from being shared outside the practice for purposes other than direct care. After the introduction of the national data opt-out, the collection including the count of Type 1s stopped in November 2018.

[28] See Understanding Patient Data’s summaries of public attitudes research at https://understandingpatientdata.org.uk/

[29] https://sciencewise.org.uk/

arrangements needed to comply with COVID-19 safety restrictions, these are planned to take place in autumn 2020.

The intention is to ensure that the users of social care services and carers of individuals receiving social care are well represented among workshop participants because their attitudes are commonly under-researched. Following the workshops, the NDG intends to develop guidance to help organisations across the health and social care sector to carry out public benefit assessments with greater consistency and with confidence that they are in line with public values.

2.2 Priority: Encouraging information sharing for individual care

Summary of progress

Guidance for health and care staff

What we said we would do:

"We will work with others to develop advice and guidance for health and care staff with the aim of improving information sharing for individual care. This will include work to address the interplay between the requirements of common law and statutory data protection law. We will work with relevant bodies to do this, in particular the Information Commissioner's Office (ICO)."

What we did:

- We contributed to a wide range of advice and support to ensure that health and care data was shared appropriately during the COVID-19 emergency. We made clear that information may need to be shared more quickly and more widely across organisations than normal. However, there had to be safeguards to maintain public trust.
- Before COVID-19 struck we conducted a survey of professionals which found widespread concern that the laws governing data sharing are complex, poorly understood, and difficult to navigate.

Training programmes

What we said we would do:

"We will work with training and education bodies to ensure advice and guidance about information sharing is embedded into their programmes where possible."

What we did:

- We supported initiatives taken by the UK Caldicott Guardian Council (UKCGC), which provides advice to more than 18,000 Caldicott Guardians across the health and care sector.
- The UKCGC work included publishing guidance on tracing a missing person and regional workshops to support and educate Caldicott Guardians.
- We used the findings of our survey about information sharing to develop recommendations for the education and training of health and care staff.

Priority progress in-depth

Guidance for health and care staff

What we said we would do:

“We will work with others to develop advice and guidance for health and care staff with the aim of improving information sharing for individual care. This will include work to address the interplay between the requirements of common law and statutory data protection law. We will work with relevant bodies to do this, in particular the Information Commissioner’s Office (ICO).”

Supporting the COVID-19 response

The NDG’s work on developing advice and guidance gained added significance during the COVID-19 pandemic. Section 2.1 of this report has already explained the importance of transparency in maintaining trust during the emergency response. Here we expand on some advice and support to which the NDG contributed in order to make sure that appropriate data sharing was put in place rapidly during the crisis.

Dame Fiona said on April 3: “Information sharing must be done differently to support the fight against COVID-19 and to protect citizens compared to ordinary times. Information may need to be shared more quickly and widely across organisations than normal, or different types of information may need to be collected and used.” However, she added: “Even in times such as these, protecting trust in confidential health and care matters. The guidance and notices issued to allow data sharing to combat the outbreak still contain appropriate safeguards: limiting the purposes for which data can be used, who can use it and the amount of time for this to occur. These are important protections that patients may be glad to hear about.”

The NDG supported the issuing of a notice under existing legislation[30] to give the system the confidence and a clear legal basis to share information to combat the pandemic. She provided support to organisations such as the Confidentiality Advisory Group, NHS Digital and NHSX to ensure COVID-19 data requests can be dealt with quickly, but with safeguards still in place.

The NDG worked with NHSX, the Information Commissioner’s Office and others to support the development of advice about safe use of data. Guidance was issued rapidly for frontline clinicians, social care staff, volunteers and others involved in the COVID-19 response. For instance, it became clear that COVID-19 patients were much more reliant on using technology such as FaceTime and videoconferencing while isolated from their families in hospital. This could bring confidentiality risks, for instance where a patient might accidentally include images of other patients on a mobile phone call. The NDG supported NHSX to ensure guidance about the use of mobile phones in hospitals[31] was issued in a timely manner.

The NDG was also involved in discussions about how to ensure that information in patients’ Summary Care Records (SCR) was being appropriately shared during the COVID-19 pandemic. SCRs are an electronic record of important patient information, created from GP medical records. They can be seen and used by authorised staff in other areas of the health and care system involved in the patient's direct care. The SCR holds important information about current medication; allergies and details of any previous bad reactions to medicines; the name, address, date of birth and NHS number of the patient. Additional information, such as details of long-term conditions, significant medical history, or specific communications needs, may be added to the SCR and shared at the patient’s discretion. To help the NHS to respond to the coronavirus (COVID-19) pandemic, it was suggested that this additional information be included in

---

[30] https://www.gov.uk/government/publications/coronavirus-covid-19-notification-of-data-controllers-to-share-information

[31] https://www.nhsx.nhs.uk/covid-19-response/data-and-information-governance/use-mobile-devices-patients-hospitals-eg-phones-tablets-and-cameras/

Summary Care Records for patients by default, unless they had previously opted out. The NDG advised that it was proportionate and within patients' expectations that the extra detail provided in the SCR with Additional Information would be available to health professionals treating individuals. The SCR system was adjusted so that this happened.

Many of the arrangements that have been put in place for COVID-19 are temporary and due to expire later this year or when the pandemic is past. The NDG will have a role to play in reviewing these arrangements – judging what has worked, which changes should be reversed, and which should be kept in place. The NDG anticipates that there will be much to learn.

NDG survey: identifying the barriers to data sharing for direct care

Before COVID-19 struck, the NDG's main initiative on information sharing centred on work led by Dr Alan Hassey, a member of her panel. He devised an online survey to identify the barriers that are impeding effective information sharing among the professionals involved in a person's direct care. Section 2.1 of this report gave an account of one aspect of this research, namely the extent to which giving people better access to their own records might encourage better sharing among the professionals. This section turns to other findings from the survey, which ran from 23rd December 2019 until 2nd February 2020. It included a questionnaire that was completed by 65 organisations and individuals engaged in this field.

The survey found that those working in the system feel that the laws that govern data sharing are so complex, poorly understood, and difficult to navigate that they do not have confidence to do so. It suggested that patients and social care service users may be suffering as a result. Relevant information about them is often not being shared appropriately and not being made available at the point of care. Respondents highlighted how, with the further blurring of boundaries between clinical and non-clinical elements of teams supporting people (through activity such as population health management), this environment is becoming ever more complex and the need for clear guidance and support in this area will only grow.

A recommendation based upon the survey's findings called on key stakeholders to develop an education and training strategy to encourage information sharing for individual care. There needs to be clarity about what falls within direct care and what does not. Any new guidance needs to use clear language and be consistent with a changing health and care landscape. Patients and service users should be able to access important information about their health and care in ways that help them understand the content and context of that information. The access to information by care staff and carers is important too. There needs to be a common understanding among stakeholders of what specific data and information is required by the health and care system to meet the different demands of care provision, research and planning. This should be combined with an increased focus on data quality, structure and access hierarchies. This would enable the relevant data (and *only* the relevant data) to be accessed by the appropriate teams and at the appropriate points, without the issues that could be caused by the sharing of the entire patient record.

The NDG will be publishing the report in August 2020 and will work with other system stakeholders with the aim of ensuring that these recommendations are taken forward to improve information sharing and to empower patients.

Formal system-wide review of existing guidance

The NDG, as a member of the Health and Care Information Governance Panel[32] (HCIGP), has agreed that she will be part of a process of ensuring that information governance advice given to the system is consistent and coordinated. The HCIGP is convened by NHSX and includes the ICO, NHS Digital, Health Research Authority, Care Quality Commission, Public Health England and others.

---

[32] The HCIGP was established to support the co-ordination of the provision of strategic IG advice to the health and care system. Its role is to advise and support NHSX in the development of strategic IG advice and provide expert input and reflection as requested.

The NDG, ICO and NHSX had planned to get this review underway by bringing together a range of other stakeholders to discuss what its priorities should be. The relevant meetings and communications had to be postponed due to the COVID-19 outbreak. The NDG will be working with the panel to review existing guidance and produce new guidance.

The NDG also looks forward to continuing to contribute to the work that the ICO has started, to produce new anonymisation guidance to replace its Anonymisation Code of Practice. This project, which will be important and significant for the health and social care sector, has also been affected by COVID-19.

Local Health and Care Record programme

During 2019-20 the NDG was involved in reviewing and providing feedback on several iterations of an information governance framework for the Local Health and Care Record (LHCR) programme. The LHCRs are regional collaborations of NHS organisations and local authority social care departments that are being formed to encourage information sharing to improve health and care and people's experience of it. Initially they will share information about patients and service users for direct care purposes within a LHCR region. Subsequently, NHSX wants them to share for direct care across LHCR boundaries and also to share de-identified data for other purposes such as population health management and research. The NDG has been represented on a steering group of stakeholders that advised NHSX on a framework to help the LHCRs comply with data law and public expectations.

Training programmes

What we said we would do:

"We will work with training and education bodies to ensure advice and guidance about information sharing is embedded into their programmes where possible."

The NDG made recommendations to the Health and Care Information Governance Panel on embedding advice on information sharing into training and education programmes, as reported above.

Supporting UK Caldicott Guardian Council initiatives

In addition, the NDG supported a series of initiatives taken by the UK Caldicott Guardian Council (UKCGC), which provides advice to more than 18,000 Caldicott Guardians in organisations across the health and care sector. These organisations include NHS providers and commissioners, GPs, social care departments in local authorities, charities, hospices and other services for patients and service users. Dr Chris Bunch, chair of the UKCGC, attends the NDG's Panel meetings and the Office of the NDG provides the secretariat and support for the UKCGC's work.

A Caldicott Guardian is a senior person within a health or social care organisation who makes sure that the personal information about those who come for its services is used legally, ethically and appropriately, and that confidentiality is maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing. They are often described as the conscience of their organisation.

NHS organisations have been required to have a Caldicott Guardian since 1998[33], and local authorities providing social care in England have been required to do so since 2002[34].The requirements were promulgated in departmental circulars and there has been no statutory basis for the role. However, over recent years, organisations handling NHS confidential patient information were required to complete NHS Digital's Information Governance Toolkit (IGT), which required details of each organisation's Caldicott Guardian, making the role effectively mandatory. The new Data Security and Protection Toolkit (DSPT), which replaced the IGT, only requires Caldicott Guardian details for NHS organisations.

During 2019-20 the UKCGC used data from the DSPT and the Caldicott Guardian Register maintained by NHS Digital to compile the first full list of Caldicott

---

[33] Health Service Circular 1999/012

[34] Local Authority Circular 2002/2

Guardians across the UK. Once the appropriate governance and opt-out arrangements were in place, the UKCGC circulated a newsletter to raise awareness of the support available to Caldicott Guardians and help to distinguish them from other roles in the current health and care landscape.

The next stages for this work are to provide further helpful content via the newsletter, signpost to the support available and help to clearly define and establish the role and responsibilities.

Since 2008, all NHS organisations processing NHS patient information have been required to have a Senior Information Risk Owner (SIRO). Since 2018 all public authorities[35] have been required by the General Data Protection Regulation[36] and the Data Protection Act (2018) to appoint a Data Protection Officer (DPO). Although the SIRO and DPO roles are distinctly different from that of the Caldicott Guardian, there are overlaps that seem to cause confusion. The UKCGC is leading a piece of work to ensure that the role of Caldicott Guardians remains clear and distinct.

The UKCGC has obtained ownership of the Caldicott Guardian training materials from NHS Digital as part of its programme to raise the education levels of Caldicott Guardians across health and care; it also works with a number of training providers across the UKCGC to ensure that appropriate topics are covered. The UKCGC runs regular regional workshops to support and educate Caldicott Guardians. It often helps the Office of the NDG to investigate and respond to cases and enquiries that it receives; they are often the most appropriate group to handle specific queries.

During 2019-20 the UKCGC was invited to be part of the review of the Data Security Awareness – Level 1 training, which increased the focus on cyber security in response to the WannaCry ransomware attack in May 2017. Working with colleagues from NHS Digital, Health Education England (HEE) and e-learning for health (e-lfh), they were able to ensure that the importance of the Common Law Duty of Confidentiality and the Caldicott Principles were maintained in the Level 1 training.

In May 2019, an article published on the UKCGC website[37] provided guidance on when it is appropriate to enable the police to access health and social care information to help trace a missing person. Sandra Lomax, the UKCGC vice-chair, worked with the National Crime Agency to establish guidelines that should be borne in mind when information is being sought from health and care. They made clear the sort of information that the police should provide upfront, and also described the legal bases that underpin and allow such information sharing.

During 2019 the UKCGC stored details of all the enquiries it received, with a view to publishing a helpful catalogue of anonymised scenarios and factors a Caldicott Guardian should consider to reach a decision. This work continued into 2020-21.

---

[35] Those considered a public body under the Freedom of Information Act

[36] Article 37, Recital 97

[37] https://www.ukcgc.uk/news/2019/5/22/sharing-information-with-the-police-to-help-trace-missing-persons-the-process-considerations-and-legal-basis

2.3 Priority: Safeguarding a confidential health and care system

Summary of progress

Reasonable expectations

What we said we would do:

"We will progress the concept of reasonable expectations and provide an update on our next steps."

What we did:

- We developed proposals for an additional Caldicott Principle, emphasising the importance of considering and informing citizens' reasonable expectations when using and sharing confidential information.
- We held a workshop with regulators and stakeholders which demonstrated strong support for these proposals.
- After deliberating on what we heard, and further discussions with stakeholders, we decided to consult on the wording of this eighth Caldicott Principle, some rewording of the existing seven principles, and on a proposal that the NDG uses her statutory power to issue guidance about Caldicott Guardians.

Protecting confidentiality

What we said we would do:

"We will continue other work under the broad 'safeguarding confidentiality' theme. This will include work to ensure confidential patient information is not inappropriately linked with other types of data and/or used for non-healthcare purposes in a manner that could undermine public trust and, potentially, discourage individuals from seeking healthcare."

What we did:

- We continued to advise the Department of Health and Social Care and arm's length bodies on implementation of the 10 data security standards that were recommended in the NDG's 2016 Review of Data Security, Consent and Opt-outs.
- We engaged with the Care Quality Commission and NHS Digital to help them improve the monitoring of organisations' compliance with those standards. They are working together to develop a more intelligence-driven approach.
- The NDG supported NHS Digital's campaign to help staff understand more about cyber security threats and what they can do to reduce them.
- Our work on challenging poor practice included consideration of a pilot scheme initiated by NHS Improvement in 2019. It invited eight NHS trusts to use the credit reference company Experian to help to identify patients who did not have the right to free NHS care. We responded to a request from the Information Commissioner's Office for comment on the confidentiality aspects of the scheme. We found several grounds for concern. The pilot scheme was abandoned.

Priority progress in-depth

Reasonable expectations

What we said we would do:

"We will progress the concept of reasonable expectations and provide an update on our next steps."

The duty of confidence is fundamental to the relationship of trust between health and care professionals and those in their care. This duty under common law predated by many centuries the statute laws on privacy, including most recently the Data Protection Act 2018. It remains an important underpinning of good professional practice. Safeguarding the duty of confidence is seen by the NDG as a fundamental priority.

Her recent work on the subject was triggered by concern that some organisations were claiming they had the implied consent of service users to use and share information about them, when in fact it was *not* reasonable to expect that they knew what was happening to their data. Starting in 2017, this led to a series of seminars[38], a citizens' jury[39] and articles[40] published on her website.

That work led the NDG to the conclusion that the reasonable expectations of patients and service users should be brought more explicitly into the foreground of decision making by health and care professionals. Her thinking on this was informed by academic work led by two of her panel members, Dr Mark J Taylor and Professor James Wilson, which resulted in the publication of Reasonable *Expectations of Privacy and Disclosure of Health Data*[41]. This article demonstrated that since the Human Rights Act 1998 came into force, courts have developed the significance of the concept of a 'reasonable expectation of privacy' within the law of confidence. It argued that one result of this is to provide an alternative route for the lawful disclosure of confidential patient information, where there is no reasonable expectation of privacy in all the circumstances of the case.

An eighth Caldicott Principle

The NDG had long espoused the maxim that there should be "no surprises" for patients and service users. However, the seven Caldicott Principles did not specifically include this point. This raised the question about whether there should be an eighth Caldicott principle to foreground the matter.

That suggestion was one of the main propositions put to an NDG workshop on 4th February 2020 attended by key regulators and stakeholders. Using interactive polling, the event demonstrated strong support for the creation of an eighth Caldicott principle making clear that patients' and service users' expectations must be considered and informed when confidential information is used.

The NDG believes that a number of benefits would result from the introduction of the new principle. It would:

- Be consistent with the direction that the courts have taken in making the reasonable expectations of the individual the touchstone of the duty of confidentiality.
- Add explicit reference in the principles to the NDG's long-standing view that there should be 'no surprises' for the public in regard to the use of their confidential information in order to build public trust.
- Align with the GDPR emphasis on transparency and data subject rights.
- Align with professional guidance such as the General Medical Council's

---

[38] https://www.gov.uk/government/publications/sharing-data-in-line-with-patients-reasonable-expectations

[39] https://www.gov.uk/government/speeches/talking-with-citizens-about-expectations-for-data-sharing-and-privacy

[40] For example, https://www.gov.uk/government/speeches/reasonable-expectations and https://www.gov.uk/government/speeches/exceeding-expectations

[41] Taylor, M.J. and Wilson, J., 2019. Reasonable Expectations of Privacy and Disclosure of Health Data. Medical Law Review, 27(3), pp.432-460

Confidentiality: good practice in handling patient information.

- Reflect the welcome move in recent years away from paternalism in care and towards a partnership approach between health and care professionals and individuals.

It is not envisaged that such a principle would establish reasonable expectations as a legal basis in its own right to meet the duty of confidence. However, given the established influence and importance of the Caldicott Principles, it is hoped that it would contribute to ensuring that the perspective of patients and service users is helpfully emphasised in decisions to use and share confidential information.

The NDG and her panel decided to consult on the wording of a new eighth principle and take the opportunity to present some proposed rewording of the existing seven principles to ensure they remain clear and up to date.

Statutory guidance on Caldicott Guardians

The National Data Guardian will also seek views on the proposal that she issues guidance about the appointment of Caldicott Guardians using her statutory power[42].

As explained in section 2.2, NHS organisations have been required to have a Caldicott Guardian since 1998[43], and local authorities providing social care in England have been required to do so since 2002[44]. However, the requirements were promulgated in departmental circulars and there is no statutory basis for the role. It was left to individual organisations to determine how they operate.

Protecting confidentiality

What we said we would do:

"We will continue other work under the broad 'safeguarding confidentiality' theme. This will include work to ensure confidential patient information is not inappropriately linked with other types of data and/or used for non-healthcare purposes in a manner that could undermine public trust and, potentially, discourage individuals from seeking healthcare."

Implementing the NDG's data security standards

During 2019-20 the NDG and her panel members continued to advise the DHSC on the implementation of the data security standards that were recommended in her 2016 *Review of Data Security, Consent and Opt-outs*. The objective of this work was to improve cyber security across the health and care system.

The NDG also engaged with senior officials from NHS Digital and other organisations with responsibilities in this area to understand the work being undertaken to support the system to meet the data security standards. The 2016 review had highlighted the importance of organisational leadership, saying: "The leadership of every organisation should demonstrate clear ownership and responsibility for data security, just as it does for clinical and financial management and accountability." The importance of the 'people' factor in data security, had led the NDG to place these first when she shaped her recommendations around three themes of People, Processes and Technology. Her advice about, and scrutiny of, the work being done to implement the recommendations often focused on the importance of supporting leaders and their staff to do the right thing, as well as getting improvements in technology and processes in place.

The NDG was therefore pleased to endorse NHS Digital's campaign to help staff understand more about cyber security threats and what they can do to reduce risk. The campaign launched by NHS Digital's Data Security Centre aimed to educate staff across the NHS on the direct impact of data and cyber security on patient safety and care.

In her endorsement, Dame Fiona said: "We know that there is widespread commitment across the NHS to keeping

---

[42] http://www.legislation.gov.uk/ukpga/2018/31/contents/enacted

[43] Health Service Circular 1999/012

[44] Local Authority Circular 2002/2

data secure and that the public places great trust in the NHS to do so. However, we can always do more to protect against potential risks, which is why I'm pleased that NHS Digital have created their 'Keep I.T. confidential' campaign and toolkit for the healthcare workforce. It aims to educate, reinforce and improve the correct behaviours that we all need to practice both in the workplace and in our daily lives to keep information (our own and that of others) safe and confidential."

The NDG was also pleased to hear about improvements in technology to help the system maintain data security, such as the renewal of Windows licences and the implementation of Advanced Threat Protection across millions of NHS devices. In December 2019, NHS Digital colleagues attended her panel to describe its work to provide a Secure Boundary service[45] for NHS trusts and Commissioning Support Units. Panel members were interested in the potential it has for raising data security and resilience and therefore protecting patient data and services.

Adherence to the standards is assessed through the Data Security and Protection Toolkit (and associated audit regime for large NHS organisations). All organisations that have access to NHS patient data and systems should complete a Data Security and Protection Toolkit (DSPT) self-assessment annually. Cyber-security is also included in complementary Key Lines of Enquiry (KLOEs) for inspections run by the Care Quality Commission (CQC).

During 2019-20, the NDG engaged with the CQC and NHS Digital to help them develop this monitoring to better support health and care organisations. They are working together to develop a more intelligence-driven approach. The aim is for NHS Digital to review intelligence about an NHS Trust and provide an expert opinion (or even a rating) to CQC. The CQC wants to reserve the right to send an NHS Digital expert into Trusts when there was a rationale for doing so.

The normal deadline for organisations to complete their DSPT returns is 31st March. However, the deadline for 2019-20 returns was postponed in the light of the COVID-19 emergency until 30th September 2020. NHS Digital continues to publish details of organisations as they complete their DSPT assessment (via the DSPT organisation search[46]). To date 19,500 organisations have completed an assessment against the 2019-20 standard.

The NDG has been impressed by the improvements in data security that have been enabled by the work to implement the NDG standards and the recommendations of the WannaCry review[47]. She has been concerned to see that social care organisations are not left behind and are given adequate support to enable them to maintain data security. She was pleased to discuss the findings and recommendations of work led by the Local Government Association to examine the challenges faced by the social care sector and supports the recommendations of that work[48]. She was also pleased to see changes made to the DSPT to make it more relevant to the needs of the social care sector. Last year there was an increase of 160% in the percentage of social care organisations completing a DSPT return to the level that allows them to access NHSmail[49] – this is very positive, as it enabled organisations in the sector to more securely exchange information with other organisations. The NDG believes that support for social care organisations to strengthen data security will need ongoing attention.

Implementing the National Data Opt-out

In addition to checking on organisations' data security the DSPT also requires them to demonstrate a good standard of information governance. One aspect of this was that all NHS organisations in England

---

[45] https://digital.nhs.uk/cyber-and-data-security/managing-security/nhs-secure-boundary

[46] https://www.dsptoolkit.nhs.uk/OrganisationSearch

[47] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

[48] https://www.digitalsocialcare.co.uk/new-report-and-guidance-on-data-and-cyber-security-for-social-care-services

[49] Over 3,000 additional social care organisations have completed an assessment against the 2019-20 DSPT standard to date.

should have met the Government's deadline for implementing the National Data Opt-out by 31st March 2020. A consequence of postponing the cut-off date for DSPT returns in response to the COVID-19 emergency is that there is not yet reliable information on how many organisations are upholding the National Data Opt-out.

The opt-out was recommended by the NDG in her 2016 *Review of Data Security, Consent and Opt-outs*. After a public consultation, the Government accepted all the Review recommendations on 12th July 2017[50]. The National Data Opt-out has been upheld by NHS Digital since 25th May 2018 and by Public Health England since September 2018. This means that those organisations had procedures in place to stop confidential patient information about people who have opted out being used for purposes other than their direct care. To help all the other health and care organisations to become compliant, NHS Digital maintained a National Data Opt-out Programme (NDOP) unit that was due to continue work until the deadline for compliance on 31st March 2020. However, after a review of a wide range of digital services, this unit was stood down in September 2019 and the task of supporting organisations to become compliant became part of the "business as usual" of NHS Digital.

On 7th August 2019 the NDG wrote to NHSX in response to this decision. She said:

"In spite of the work that we can see has been done to prepare for the early move to a live service, we retain concerns that the many organisations which have yet to implement the opt-out may not be sufficiently supported in the run-up to March 2020 … It will therefore be important [to have] careful monitoring of the demand for NDOP implementation support, in particular as we approach the March 2020 upholding deadline, to ensure that the service is able to be responsive to organisations that must comply with the policy. It will also be important that learning from the NDOP programme is taken on board by NHSX as it discharges its responsibility for cross-system guidance on information governance."

In spite of the subsequent postponement of the compliance deadline in response to the COVID-19 emergency, implementation of the National Data Opt-out remains a clear ministerial objective.

Polling on awareness of the National Data Opt-out

Polling conducted for the NDG by the opinion research company Kantar in February 2020 found 59% of people trusted the NHS to look after data about them. This figure was higher than any other included in a list provided to respondents, which also included banks, family and friends, local and central government, insurance companies and online retailers. The same proportion agreed that allowing different NHS organisations to share patient information and data enables them to research new treatments, speed up diagnosis and improve patient care, with another 21% saying they agreed with this somewhat.

However, the poll found that only just over a third (35%) said they were aware that individual patients can opt out of sharing their confidential data for medical research and planning. This compared with 57% public awareness in a poll conducted by Kantar for the NDOP programme shortly after a six-week public information campaign to prepare people for the launch of the National Data Opt-out in May 2018. It is perhaps unsurprising that many people forgot about the opt-out when it was no longer being publicised, but there is a case now for the message to be refreshed.

The February 2020 polling by Kantar found that, once told about the opt-out, around a quarter of people (26%) said that they were likely to opt-out. Health and social care staff were much more likely to say they were likely to opt-out. Among people working in health and care, nearly half (45%) said that they would opt-out.

Challenging poor practice

The NDG is often called upon to look into cases where best practice appears not to have been followed. One example came in 2019 as a result of an NHS Improvement pilot, involving the credit reference

---

[50] https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care

company Experian. NHS Improvement invited eight NHS Trusts to join a pilot scheme that would have seen them providing Experian with details of patients' name, address, date of birth and a unique identifier. Experian would then use its resources to establish whether these individuals had “an economic footprint” in the UK – a likely indicator of UK residence, which the trusts would then be able to use to identity which patients might not be entitled to free healthcare because they were not ordinarily resident in the UK.

The pilot would have had similarities to a scheme that had been running since 2015 in south-east London where Lewisham and Greenwich NHS trust used Experian to help it determine which patients might not be eligible for free NHS care.

The NDG was asked by the Information Commissioner's Office to comment on the confidentiality aspects of the proposal. The NDG replied: “My Panel and I are clear that patients would usually have a reasonable expectation of privacy with regard to such information held by a hospital trust. The duty of confidentiality should be understood to apply, and a common law justification is therefore needed for the use of such data. In this case, the use is clearly beyond the provision of individual (direct) care and so the legal basis would need to be appropriate to this...

“We find it hard to anticipate how, even if clear and accessible information were made available to patients, trusts taking part in the pilot proposed would have been able to rely on an appropriate legal basis for meeting their confidentiality obligations. One fundamental difficulty is that it is not clear that such a use of data could have been demonstrated to be proportionate and effective...

“With regards to public trust, our impression is that the potential negative impacts of the pilot were not well anticipated. When individuals disclose information to health and care professionals, they do so within the context of a relationship of trust. To protect this relationship, it is essential that patients and service users' confidential information is used in ways that they expect and accept. If this trust does not exist, individuals may avoid seeking help or under-report symptoms.”

Ultimately, only one NHS Trust took part in the pilot, but it did not act on the data file received from Experian. The pilot was halted. Lewisham and Greenwich NHS Trust stopped using Experian in September 2019. One of its directors subsequently told Lewisham Council's healthier communities select committee that he “struggles to defend the logic” behind the decision to use Experian in the way that it was.

Digital Economy Act and information sharing power

The NDG is represented on the Public Service Delivery Review Board, which was set up by the Digital Economy Act (DEA) 2017 under the leadership of the Department for Digital, Culture, Media and Sport (DCMS)[51]. The Review Board oversees usage of the public service delivery data sharing power (chapter one of Part 5 of the DEA).

As a result of public and stakeholder consultation at the time of the DEA passing through Parliament, health and adult social care bodies were not included in the list of specified bodies permitted to use the powers.

The NDG was still carrying out her review of data security, consent, and opt-outs[52] at the time the DEA was going through Parliament in 2016. The Government response to its 2016 Better Use of Data consultation, which looked at how data sharing powers should be used, said[53]:

“Health and care data plays a critical role in the design and delivery of public services and in driving improved outcomes for citizens. However, health and care data is particularly sensitive and rightly needs additional protections. For health and care data to be included, additional safeguards regarding confidential personal information are likely to be required and

---

[51] https://www.gov.uk/government/groups/digital-economy-act-public-service-delivery-review-board
[52] https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs
[53] https://www.gov.uk/government/consultations/better-use-of-data-in-government

we need to ensure these are in line with Dame Fiona Caldicott's review due in early 2016. Cabinet Office and Health officials will work together to explore ways in which health and care data may be integrated into the proposed legislation in a way that incorporates an extra layer of safeguards consistent with Dame Fiona's recommendations."

Any move to bring health and care data into scope would first require public consultation, including with appropriate representative health bodies, adult health and social care bodies in England and then affirmative regulations to be made in Parliament.

As set in the NDG's priorities, Dame Fiona believes that care should be taken with any proposal that confidential patient information is used for non-healthcare purposes. It is critically important individuals should not be discouraged from seeking healthcare or confiding frankly in their care professionals for fear that their information may be used for non-healthcare purposes they do not support.

Guidance for those developing data driven technologies

The NDG has supported work by the Health Research Authority (HRA) to update guidance helping organisations understand how they can use data when designing, developing, and testing new data-driven technologies.

A significant impetus for the updating of this guidance was learning from the Information Commissioner's Office's investigation into the decision by the Royal Free London NHS Foundation Trust to provide large quantities of patient data to DeepMind Health, then a UK subsidiary of Google, to develop and test an app, known as Streams, to track acute kidney injury[54]. Statements on the case by the ICO, NDG and HRA all pointed to the need for clearer guidance to support the safe and appropriate use of data in innovation.

The new guidance, which is due for publication soon, will summarise the information governance and regulatory approval requirements where patient data is used in data-driven technologies in the NHS and adult social care. It will be aimed at helping those involved in research and manufacturing of data-driven technologies, as well as those in health organisations who are responsible for the safety, deployment, and ongoing monitoring of data-driven technologies.

The new guidance will replace and augment the Clinical Safety Guidance available from NHS Digital[55]. The new guidance will be endorsed by a number of stakeholders. It will go through the NHSX health data guidance process and will be kitemarked by the National Health and Care Information Governance Panel and published on the NHSX portal.

---

[54] See page 21 of the NDG's Progress Report: January 2018 to March 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/823491/NDG_progress_report_2018-19_v1.0_FINAL__002_.pdf

[55] This guidance is available at https://digital.nhs.uk/services/solution-assurance/the-clinical-safety-team/clinical-safety-documentation

3 Work priorities

This year’s priorities remain the same as those set out in last year’s NDG progress report. We explained then that her priorities (drafted following a public consultation[56]) would require ongoing work in the coming years for many organisations working together.

It also made clear that delivering the priorities would not to be the NDG’s only work. She will continue to respond to the requests for advice and guidance that she receives from members of the public, Government and its agencies, health and social care organisations, researchers, professional bodies and more.

Supporting public understanding and knowledge

- We will work with the relevant bodies to explore the barriers to improving patient access to their records and to information about how data about them has been used.
- We will continue to champion the NDG’s long-standing principle that those using and sharing data must be transparent and that they must engage with the public and patients so that the case for data sharing is made.
- We will examine what additional public engagement would be most useful on the subject of the benefits from the use of health and care data.
- We will continue to support the work to develop a framework to realise the benefits for patients and the NHS where health and care data is being used to underpin innovation.

Encouraging information sharing for individual care

- We will work with others to develop advice and guidance for health and care staff with the aim of improving information sharing for individual care. This will include work to address the interplay between the requirements of common law and statutory data protection law. We will work with relevant bodies to do this, in particular the Information Commissioner’s Office (ICO).
- We will work with training and education bodies to ensure advice and guidance about information sharing is embedded into their programmes where possible.

Safeguarding a confidential health and care system

- We will progress the concept of reasonable expectations and provide an update on our next steps.
- We will continue other work under the broad ‘safeguarding confidentiality’ theme. This will include work to ensure confidential patient information is not inappropriately linked with other types of data and/or used for non-healthcare purposes in a manner that could undermine public trust and, potentially, discourage individuals from seeking healthcare.

---

[56] https://www.gov.uk/government/consultations/national-data-guardian-a-consultation-on-priorities

4 Financial statement

2019-2020

The National Data Guardian (NDG) is a non-incorporated office holder, who does not, herself, employ staff, hold a budget, or produce accounts.

The Department of Health and Social Care (DHSC) holds the budget (which was £700,000 in 2019/20) to meet the costs of:

- The Office of the NDG (salaries, accommodation, IT equipment etc).
- The work of the NDG, her advisory panel, and the work of the associated UK Caldicott Guardian Council.
- Events, public engagement, additional staff training etc.

NDG staff breakdown

The Office of the National Data Guardian is hosted by NHS Digital.

For 2019-20, the staffing breakdown for National Data Guardian staff includes the below roles and their associated NHS Agenda for Change pay bands:

• Head of the Office of the NDG	8c
• Senior Project Manager	8b
• Senior Policy Advisor	8b
• Communications Manager	8a
• Business Support Manager	6

The NDG, as an independent post-holder, has the flexibility to allocate spending according to in-year priorities.

Expenditure is reported through the DHSC Annual Report and Accounts.

5 Appendix

List of National Data Guardian panel members

NDG panel members during 2019-20:

- Mike Adams (Royal College of Nursing Director, England)
- Dr Joanne Bailey (former GP, tribunal member (Social Entitlements), clinical ethics tutor)
- John Carvel (Non-Executive Director, Dorset HealthCare University NHS Foundation Trust)
- *Mark Golledge (Local Government Association) – no longer in post*
- Dr Alan Hassey (retired GP)
- *Dame Donna Kinnair (Royal College of Nursing) – no longer in post*
- *Patricia Marquis (Royal College of Nursing) – no longer in post*
- Rakesh Marwaha (former commissioning accountable officer
- Eileen Phillips (freelance writer, communications consultant)
- Professor Martin Severs (Chief Medical Officer at Zesty; former Caldicott Guardian / Lead Clinician, NHS Digital)
- Rob Shaw (Managing Director at Mercury Technology Ltd; former Deputy Chief Executive, NHS Digital)
- *Anne Stebbing (Hampshire Hospitals NHS Foundation Trust) – no longer in post*
- David Watts (Director of Adult Services, City of Wolverhampton Council)
- Dr James Wilson (senior lecturer in the Department of Philosophy at University College London)