NDG National Data Guardian
for health and social care

The National Data Guardian for Health and Care

Progress Report: January 2018–March 2019

Published 1ST August 2019

Contents

Foreword by Dame Fiona Caldicott

At a time of accelerating change across health and care it is more important than ever to hold firm to fundamental principles. It is now over 20 years since the Government asked me to lead an inquiry into how people's health data should be handled by the NHS. The Caldicott Committee's Review of Patient Identifiable Information was commissioned when the NHS was starting to implement a move from paper to computerised records, with the result that information could be sent much more easily from one part of the health service to another.

Our report in 1997 highlighted the benefits of what we called an "information explosion". For patients and clinicians the improved flow of information offered the prospect of more effective and efficient care; for clinicians and managers it also provided better evidence for planning and monitoring services. However, the 1997 report also acknowledged a tension. On the one hand there was an understandable desire among those running and planning services to use patient information in novel ways. But on the other, there was the danger that such novelty might conflict with patients' awareness and expectations concerning how information about them would be used. The review said that managing that tension by "adhering to explicit and transparent principles of good practice" will "reassure patients and those treating them that confidentiality is safeguarded" and that "patients expect nothing less."

I looked back at the 1997 report while considering what should be the National Data Guardian's first set of priorities since gaining statutory authority. What struck me was how little the arguments have changed. The "information explosion" has become many times more powerful and the technology of today presents even more exciting opportunities to provide better, safer, more individualised care. However, we face a similar tension, which we must address, to facilitate desirable innovation without conflicting with public expectations about how health and care data will be used.

Now, as then, we have to work with the public's views. Confidentiality remains as important as ever. People need to be able to tell their doctor, nurse, or care worker things about themselves and their health and care needs in confidence. If such information is then used in a way that patients and service users do not expect, this precious trust will be undermined and the essential willingness of people to confide in those they consult will be reduced.

An ongoing conversation with the public is essential. This must be a two-way dialogue, in which people's expectations are both listened to and informed. We also need to reassure the public that there are strong safeguards in place to protect personal confidential data securely.

Just as was the case 20 years ago, I believe we can earn public support for the use of data in innovation, by "adhering to explicit and transparent principles of good practice" to "reassure patients and those treating them that confidentiality is safeguarded". Now as then, the public rightly expects nothing less.

In this report I outline the work that my Panel and I have carried out since January 2018 to uphold those principles. I would like to thank all the people who have helped us in that important task. As we now join with our colleagues across the system to deliver our new priorities, we will continue our efforts to ensure that the rights of patients and service users are respected, and their voices are heard.

Dame Fiona Caldicott
MA FRCP FRCPsych
National Data Guardian
for Health and Social Care in England

Section 1. Overview and summary

Never before have people been so aware of the power of information science to affect their lives – for good and for ill. In health and care the ability to assemble and interpret data is creating valuable new opportunities to save lives and improve personal welfare. Artificial intelligence and machine learning are starting to revolutionise clinical practice, allowing rapid interpretation of scans and test results to supplement the clinical skills of professionals. Advances in genomics are opening up possibilities for a new generation of individualised medicine. In many parts of England, shared record schemes giving doctors, nurses and social workers rapid electronic access to the medical notes of people in their care are saving lives and improving the quality of services.

Yet the power of data sometimes also creates alarm. Across the world, organisations have been found vulnerable to cyber-attack by criminals, sometimes supported by foreign governments. Social media giants and other large corporations have faced criticism for failing to respect their customers' privacy.

It is especially important in the field of health and social care that people can trust that their confidential information is securely safeguarded and used wisely. Patients and service users need to be able to talk frankly to their doctor, nurse or social worker without fear that their privacy may be compromised.

The NHS has an unrivalled collection of datasets that can be used to develop sophisticated tools to improve healthcare management and develop new treatments. But the data must only be used in ways that do not erode people's trust. That requires maximum transparency to minimise the risk that people may be unpleasantly surprised at how their data has been used. It is the mission of the National Data Guardian for Health and Social Care (NDG) to advise and challenge the health and care system to ensure that it remains trustworthy in this respect.

On 20th December 2018 Royal Assent was received for a law to place the role of the NDG on a statutory footing. This gives the NDG the ability to issue guidance about the processing of health and adult social care data in England. Public bodies, such as hospitals, GPs, care homes, planners and commissioners of services, will have to take note of guidance that is relevant to them. So will organisations such as private companies or charities which are delivering services for the NHS or publicly funded adult social care.[1]

This law came into operation on 1st April 2019 and Matt Hancock, the Secretary of State for Health and Social Care, appointed Dame Fiona Caldicott to become the first statutory NDG. For her, this represented a continuation and enhancement of the work she had been doing since November 2014 when Jeremy Hunt, the previous Secretary of State, appointed her as the (non-statutory) NDG, pending Parliamentary approval of formal powers. He asked her to be "the patient's champion" upholding the security of personal medical information and raising concerns publicly about improper data use.[2]

The foundation for her work in this field was the Information Governance

[1] http://www.legislation.gov.uk/ukpga/2018/31/contents/enacted/data.htm
[2] https://www.gov.uk/government/speeches/innovation-and-efficiency?utm_source=twitter&utm_medium=social

Review[3] 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 she delivered to the department in 1997[4]. 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[5].

Dame Fiona published a subsequent account in December 2017 describing her work as NDG during 2015-17 and setting eight priorities for 2018[6]. This present report resumes that narrative, describing activity under each of the priority headings. By doing so it completes the record of what was achieved before the statutory powers came into operation. Under the Act there is a requirement to produce annual reports and it is anticipated that these will be laid before Parliament during the summer in future years.

During the period covered by this report the NDG has been supported by a small team of officials and a panel of independent advisers. The Panel's terms of reference are provided in Appendix C and its membership is in Appendix B. The minutes of its deliberations are available on the NDG's webpages.[7]

Section 2 of this report examines what was done in 2018-19 to address the NDG's eight priorities. These were:

Priority 1. To support the successful implementation of the NDG Review's recommendations in full, providing advice and challenge where appropriate to those tasked with their implementation.

During 2018-19 the NDG and her Panel contributed to the work led by the Department of Health and Social Care (DHSC), NHS Digital and NHS England to implement the recommendations of her Review of Data Security, Consent and Opt-outs. The National Data Opt-out was launched in May 2018, allowing people to opt out of their confidential patient information being used for purposes beyond their individual care. NHS Digital and Public Health England are now compliant with the opt-out and have procedures in place to stop data about those who have opted out being used for research, planning NHS services and other purposes beyond the individual's direct care. NHS trusts and other organisations are required to be compliant with the opt-out by March 2020.

The launch came on the same day as changes to UK privacy law caused by application of the General Data Protection Regulation. This hugely important development, affecting all sectors of activity, tended to overshadow a well-prepared communications campaign to help the public understand the introduction of the opt-out for health and care. As a result, the launch campaign did not stimulate as much public discussion about the use of health and care data as the NDG had anticipated when she wrote her Review. For the NDG, encouraging this public conversation remains work in progress.

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

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

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

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

[7] https://www.gov.uk/government/organisations/national-data-guardian

Other Review recommendations that were successfully implemented included tougher, criminal penalties for those who misuse patient data and a requirement on all health and social care organisations to audit their systems and practices against the NDG's 10 data security standards. By 31st March 2019 all health and social care organisations that provide care through the NHS Standard Contract were required to provide evidence of compliance with a new Data Security Protection Toolkit.

Priority 2. To support, as appropriate, putting the post of the NDG on a suitable statutory footing so that the work to provide advice to the health and social care system can continue.

It was to the credit of Parliamentarians and civil servants that the placing of the NDG on a statutory footing was accomplished so effectively during a period of great political upheaval, when the focus was on Brexit. The Bill passed through all stages in both Houses, with multi-party support and without amendment. The intentions of Parliament were clear. They were summed up in the third reading debates in the Commons by the Parliamentary Under-Secretary for Health and Social Care, Jackie Doyle-Price, and in the Lords by the Parliamentary Under-Secretary for Health and Social Care, Lord O'Shaughnessy.

Jackie Doyle-Price said: "If data and information are to be used effectively to support better health and care outcomes, it is essential that the public have trust and confidence that safeguards are in place to protect the data from inappropriate use. That is the ethos behind the establishment of the National Data Guardian. The guardian will be an independent, authoritative voice for individuals on how their data should be used. At the heart of this is the relationship between health providers and individuals, and we need to maintain an appropriate balance between safeguarding and privacy as well as underlining the serious principle of informed consent by patients."[8]

Lord O'Shaughnessy said: "The Bill is drafted widely to allow the NDG to issue guidance about the processing of health and adult social care data. This should be interpreted broadly and would allow for the NDG to produce guidance on issues that impact on the processing of health and adult social care data. This would include, for example, good practice in security standards for storing health and adult social care data. This is an example of where guidance is not strictly focussed on health and social data itself, but about the processes and issues that could impact it. Almost anything that should be taken into account when processing health and adult social care data — or which broadly has the potential to impact, affect or influence that processing — would fall within the scope of that definition."[9]

Priority 3. To work alongside others to encourage proper sharing of data in genomic medicine and to contribute to the thinking about how patients should be engaged about this.

In order to provide benefit for patients, it may be necessary for genetic data about individuals to be shared more widely than is customary for personal medical data. For example, when a doctor or scientist gets a genetic test result for patient A, they won't necessarily know the significance of that result without examining

[8] https://hansard.parliament.uk/Commons/2018-07-06/debates/0FEC92FF-4DF6-415E-A385-916EDCD2040D/HealthAndSocialCare(NationalDataGuardian)Bill

[9] https://hansard.parliament.uk/Lords/2018-12-12/debates/1065C3E8-8789-447A-838B-0AECD85C0474/HealthAndSocialCare(NationalDataGuardian)Bill

information about as many other patients as possible. The novelty of this approach requires careful explaining to patients so that their trust is deservedly maintained.

The NDG and her Panel met representatives from NHS England and Genomics England three times in 2018 to discuss the arrangements they were putting in place for patients to become adequately informed before undergoing genomic testing – and to give their consent to the use of their data. In December 2018, the NDG wrote a letter welcoming the progress that had been made. She said: "Your proposed consent model ensures transparency for patients about how their data may be used appropriately, and what choices they may make, while also allowing for clinical pathways to remain effective."

Members of the NDG's Panel also participated in the review of the Code of Genetic Testing and Insurance, published in October 2018, and gave advice to ensure clarity for patients about their rights in relation to genetic tests when they are seeking health insurance.

Priority 4. To support work to maintain public trust in a confidential health service.

The NDG has consistently emphasised the importance of public trust. During 2018-19 she intervened to maintain public trust in a confidential health service by giving advice that helped to resolve several difficult issues.

The first of these problems concerned arrangements for the Home Office to ask NHS Digital for information, derived from NHS registration records, about the latest known address of people suspected of breaching immigration law. The NDG had numerous concerns about the data sharing agreement that was set out in the Memorandum of Understanding (MoU) between the DHSC, NHS Digital and the Home Office. She explained them in a letter to Dr Sarah Wollaston, chair of the House of Commons Health and Social Care Committee, which was inquiring into this matter. After a critical report from the committee the Government announced in May 2018 that the MoU would be revised to raise the bar for the release of demographic information to the Home Office.

Other issues that attracted the attention of the NDG included:

- The ongoing case of the use of confidential NHS patient data supplied by the Royal Free London NHS Foundation Trust to help DeepMind Health, a UK subsidiary of Google, to develop an app to track acute kidney injury. In July 2017, after seeking a view from the NDG, the ICO found that by sharing the confidential data of 1.6 million patients with DeepMind using the legal basis of 'implied consent for direct care' to justify that sharing, the Royal Free had failed to comply with data protection law and should commit to changes, including an independent audit. The Royal Free commissioned Linklaters to carry out the audit, which was delivered in May 2018. The NDG expressed her fundamental disagreement with a central claim in the audit, namely that the touchstone of whether there is a breach of confidence is to be judged from the point of view of the clinician, rather than the patient.

- NDG Panel members have been contributing to the work taking place to update the NHS Code of Practice on Confidentiality 2003. The NDG believes that the Code is an important piece of guidance for health and care, as it is looked to by frontline professionals when they wish to know how to confidently use, protect and share patient information in the patients' best interest and so that patients' reasonable expectations about their privacy are met.

Priority 5. To consider how the NDG can best support the use of data in new healthcare technologies in line with patient expectations and preferences.

The NDG engaged with the Government's Office for Life Sciences[10], which in December 2018 published the second Life Sciences Sector Deal. It gave a commitment to create a central framework for realising the benefits of NHS data, underpinned by five principles. All five are important, but the NDG was particularly encouraged by two of them:

- Any commercial arrangements agreed by NHS organisations should be transparent, clearly communicated, and not undermine public trust and confidence either in the NHS or wider government data policies.
- Any commercial arrangements agreed by NHS organisations should fully adhere to all national level legal, privacy and security obligations, including in respect of the National Data Guardian's Data Security Standards.

The NDG and her Panel were also encouraged by the "tech vision" launched by Matt Hancock, the Secretary of State for Health and Social Care, in October 2018[11]. He outlined plans to introduce minimum technical standards that digital and IT systems in the NHS will have to meet in order to provide secure communication among health and care organisations, giving appropriate access to real-time data. This should improve the sharing of information among care providers. In particular the NDG was encouraged by an enhanced commitment to give patients online access to their own records, which was recommended by the Information Governance Review in 2013.

Priority 6. To continue work to explore consensus about the way that patients' reasonable expectations should influence and shape the way that data is shared to support individuals' direct care.

In 2018 the NDG joined with Connected Health Cities to commission a citizens' jury to explore people's reasonable expectations. The question at issue was when members of the public would reasonably expect confidential information about their health and care to be disclosed by the professionals caring for them and when they would expect it to be kept private.

Over three days in January 2018 a citizens' jury of 17 people explored the subject in great depth[12], assisted by expert witnesses. After assessing the results, The NDG and Dr Mary Tully, Director of Public Engagement, Connected Health Cities, concluded: "By placing the expectations of the patient at the centre of discussions about how confidential patient information may be used, by acting consistently according to well-understood professional norms, by listening to members of the public such as our jury about what they want to see and by communicating well so that people's expectations are informed, the health and care system (or indeed any data use initiative) will

[10] https://www.gov.uk/government/organisations/office-for-life-sciences

[11] https://www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care

[12] https://www.connectedhealthcities.org/chc-hub/public-engagement/citizens-juries-chc/citizens-jury-2018/

be taking steps to ensure that it is acting in a way that is trustworthy."

The NDG intends to progress the concept of reasonable expectations during 2019-20, and will aim to issue a plan outlining the next steps.

Priority 7. To continue to liaise with a range of government bodies to further NDG objectives, such as the safe and transparent use of data.

Probably the most significant development for those responsible for data during this period was the introduction of the EU General Data Protection Regulation (GDPR), which took effect on 25th May, 2018. It was incorporated into UK law by the Data Protection Act 2018 (DPA 2018). The NDG and her Panel liaised with various Government departments and other official bodies in the national GDPR working group and contributed to the advice on implications for the NHS, social care and partner organisations that was provided through the Information Governance Alliance[13].

The introduction of GDPR and DPA 2018 brought many positive developments, but they also contributed to some confusion across the health and care sector about the interplay between the Common Law Duty of Confidence and GDPR particularly regarding consent. Guidance such as that produced by the national GDPR working group has made it clear that, for GDPR/DPA 2018 purposes, clinicians and social care staff should not rely on the consent of their patients and service users as the legal basis for processing data. However, explicit consent or implied consent will still usually be required to satisfy the Common Law Duty of Confidence. The NDG is seeking the support of other bodies to provide the necessary clarification.

In July 2018 the Care Quality Commission published a review of how local health and social care systems in 20 areas were working together to support people aged 65 and over. It found that organisations:

- were prioritising their own goals over shared responsibility to provide person centred care;
- did not always share information with each other, which meant they weren't able to make informed decisions about people's care;
- were not prioritising services which keep people well at home;
- planned their workforce in isolation to other services.

The NDG wrote in August 2018 to Ian Trenholm, the CQC chief executive, saying she was saddened by the persistence of deficits in information sharing that had been identified by her Information Governance Review in 2013. She supported the CQC's recommendations to encourage organisations to work in collaboration rather than focus narrowly on their individual remits and boundaries.

Other activities under this priority included advice to the Department for Work and Pensions on collecting consent from claimants for disclosure of data about them for the purposes of administering benefit claims. The NDG also welcomed the creation of Centre for Data Ethics and Innovation, which is an advisory body set up by Government to investigate and advise on how to maximise the benefits of data-enabled technologies, including artificial intelligence (AI).

Priority 8. To encourage the improvement and development of training and education offered to health, care and information

[13] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga

governance professionals to support safe and appropriate use and sharing of data.

In 2018-19 there was a strong impetus for improved training in the safe and appropriate use of health and care data, which came as a direct result of recommendations in the NDG's 2016 Review of Data Security, Consent and Opt-outs. During the year all organisations with access to NHS patient data had to complete an online self-assessment to demonstrate that they could be trusted to maintain the confidentiality and security of personal information. One of the requirements was to show that staff were adequately trained in data security and appropriate information sharing, as evidenced by their ability to pass a mandatory online test.

By the end of March 2019 more than 30,000 organisations had registered with this new Data Security and Protection Toolkit (DSPT) and 26,800 organisations had published an assessment against the NDG's data security standards. Despite this being the first year of a new, higher standard, the number of organisations completing an assessment was up 18% when compared with the predecessor IG Toolkit (an additional 4,200 organisations). This will have a positive impact on data security across health and care.

During 2018-19 the NDG and the UK Caldicott Guardian Council worked with NHS Digital's DSPT team to ensure that the Caldicott Principles were adequately reflected in training materials, with due regard paid to the importance of information sharing among those directly responsible for an individual's care.

Other aspects of the NDG's work on education and training included liaison with the Academy of Medical Royal Colleges, which sets standards for the way doctors are educated, trained and monitored across the UK. The NDG has also engaged with the Topol Review, the Faculty of Clinical Informatics and the NHS Digital Academy. The NDG has maintained regular representation on the Data and Cyber Security Programme Board.

Section 3 of the report looks ahead to the NDG's new priorities, which are the first she has set since the acquisition of statutory powers. The NDG's proposed priorities were published for consultation on 18th February 2019 and refined in response to views expressed by respondents. Her full consultation response[14], including the new priorities, was published on the 10th July 2019.

Section 4 includes details about how the NDG's budget was spent and the arrangements that were in place to ensure the independence of the NDG, her Panel and her staff.

A series of Annexes provide further detail.

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

Section 2. Progress during 2018-19 to address the National Data Guardian's eight priorities

Priority 1. To support the successful implementation of the NDG Review's recommendations in full, providing advice and challenge where appropriate to those tasked with their implementation.

During 2018-19 the NDG contributed to the work needed to implement her proposal for a National Data Opt-out that was being led by DHSC, NHS Digital and NHS England. Although the NDG was not responsible for implementation, she and her Panel members advised on a number of policy issues and reviewed proposals for communications and public engagement.

The NDG's Review of Data Security, Consent and Opt-outs, published on 6th July 2016, had recommended that:

"There should be a new consent/ opt-out model to allow people to opt out of their personal confidential data being used for purposes beyond their direct care. This would apply unless there is a mandatory legal requirement or an overriding public interest."[15]

After a public consultation the Government accepted all the Review recommendations on 12th July 2017[16]. However, there remained a great deal of work still to be done to determine the exact wording of the opt-out and communicate it clearly to the public to provide everyone with a genuine choice.

The Review had left open the question of whether there should be one opt-out or two. It said patients and service users should be given the opportunity to stop confidential information about them being used for research and for planning work to administer and improve local services. However, the Review had heard opposing views about whether there should be a single opt-out covering research and planning, or two questions allowing people to opt-out of one, but not the other. It concluded that engagement was needed.

[15] Recommendation 11
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF
[16] https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care

With the support of the Behavioural Insights Team[17] and using evidence from a series of focus groups, it became clear to policymakers that a single question would provide the least confusing basis for people to make their choice. Over several months before the launch of the National Data Opt-out on 25th May 2018, communications materials were tested to ensure that they gave a fair reflection of the choice people were being asked to make in language that could be easily understood.

The launch was supported by a six-week public information campaign run by NHS England and NHS Digital. It included advertising on radio and in the national and specialist black, Asian and minority ethnic (BAME) press. Posters and handout packs were distributed to 227 NHS Trusts, 8,236 GP practices, 6,603 NHS dentists, 11,869 pharmacies and 152 local Healthwatch organisations. Pre and post-waves of research to evaluate impact by research company Kantar found that people thought the ads were clear and easy to understand (79%), reassuring (67%) and told people something new (62%). However, overall public awareness of the campaign was modest (22%).

There was a significant increase in the proportion of the public that were aware that patients can opt out of sharing their confidential information for medical research and planning, from 45% in the pre-wave to 57% in the post-wave. Respondents who recognised the campaign when prompted were more likely to know that patients can opt out of sharing their confidential information (75%, compared with 53% of those who did not recognise the campaign).

It was disappointing that the launch of the opt-out did not provoke as much public discussion as the NDG had wanted. Making an opt-out available was never intended to encourage people to opt out. It was hoped that the launch would stimulate a conversation with the public that would help people to become better informed about how their data is used. Better information was to be the foundation for stronger public trust.

The launch of the National Data Opt-out came on the same day as the changes to UK privacy law caused by application of the General Data Protection Regulation. The coincidence was deliberate since policymakers sensibly decided that separate launches on different dates just a few weeks apart would have been confusing for the public. However, the consequence of the simultaneous launches was that the prepared opt-out communication material and messaging became less visible. The case for encouraging a national conversation about health and care data remains strong and the NDG hopes there may be other opportunities for it to be encouraged.

The National Data Opt-out Programme set up an online and contact centre service for people to learn more about how data is used and safeguarded and how to register a preference. Up to 31st March 2019, 12,917 choices have been made through the service, including those setting a new opt-out, and those reversing a previously set opt-out. The effect is that in total 1,639,305 opt-out patient choices are being upheld.

The total number of opt-outs is linked to a decision by ministers about how to protect the position of people who had previously registered a “Type 2” opt-out with their GP. The Type 2 opt-out was introduced by the Department of Health in 2014 in response to public concern about the care.data programme’s plan to extract data from GP records and combine it with other data held by NHS Digital. Ministers gave a commitment that identifiable data about people registering a Type 2 would not be released by NHS Digital for any reason beyond the individuals’ own care. This Type 2 opt-out survived the abandonment of the care.data

[17] https://www.bi.team/

programme in July 2016. During preparations for implementing the National Data Opt-out, ministers announced that all Type 2 opt-outs would be converted automatically into National Data Opt-outs at launch. This has had the effect that the 'opening balance' of National Data Opt-outs started at about 1.6 million. Individuals who had a Type 2 opt-out received a letter after the launch of the National Data Opt-out, informing them that their previous Type 2 had been converted to become a National Data Opt-out and directing them to the new communications about the National Data Opt-out for more information. During the first three months of its operation, 39% of all people who used the opt-out service did so to reverse an old opt-out. This was testimony to the well-considered communications, and the clear materials developed to help people better understand data sharing and their choices in respect to it.

Any further Type 2 opt-outs set during the transitional period at GP Practices that ran until 11 October 2018 were also converted.

There is a further category of patients who registered a "Type 1" opt-out preventing their identifiable data being released outside of the GP practice for purposes beyond their direct care. The Government Response to the NDG Review consultation gave the commitment that these Type 1 objections will continue to be honoured until 2020, pending full engagement with primary care professionals and the public and consultation with the NDG.

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 have procedures in place to stop confidential patient information about people who have opted out being used for purposes other than their direct care. The Department has set out that all health and care organisations need to be compliant with National Data Opt-out policy by March 2020.

In January 2019 ministers announced that the National Data Opt-out would not apply to the Cancer Patient Experience Survey[18] and other national patient surveys. Cancer charities and others had argued that automatically eliminating about 1.6 million people from survey data would jeopardise improvements in care. The NDG acknowledged the public interest in allowing individuals to be given the choice of taking part in these important NHS surveys, while ensuring that it is clear to all patients when health and care information about them will be used and in what circumstances they can opt out.

In 2018-19 the Department for Digital, Culture, Media and Sport took action to implement an important recommendation in the NDG's Review, in which she called for tougher sanctions for those who misuse data, including criminal penalties for deliberate re-identification of individuals.

On 14th September 2017 Matt Hancock, then Secretary of State at the Department for Digital, Culture, Media and Sport, wrote to the NDG, explaining that his Data Protection Bill would include a new offence of intentionally re-identifying data that has been de-identified without the consent of the controller who de-identified it. He said: "This should give patients greater confidence that if they participate in research projects, their data will be protected. I hope that you will agree this is a positive development." The NDG did agree and was reassured to see the new offence[19] introduced in the Data Protection Act which came into force in May 2018.

Cyber security

[18] https://www.england.nhs.uk/statistics/statistical-work-areas/cancer-patient-experience-survey/
[19] https://www.legislation.gov.uk/ukpga/2018/12/section/171

During 2018-19 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. It included engagement with NHS England over its report into how health and care organisations responded to the WannaCry ransomware attack on 12th May 2017[20].

This NHS England report by Will Smart, Chief Information Officer for the Health and Social Care System, said: "In July 2016, the National Data Guardian published 10 data security standards, which have been designed to address basic cyber vulnerabilities. Adherence to these standards by the health and care system could have significantly mitigated the impact of the WannaCry attack on our services. The NHS will now actively ensure that these standards are embedded across the service as part of a longer-term improvement strategy."

This strategy included strengthening of the Information Governance Toolkit to require all health and social care organisations to audit their systems and practices against the NDG's data security standards. In April 2018 the Information Governance Toolkit was replaced by a new Data Security Protection Toolkit (DSPT), which required adherence to those standards and to complementary Key Lines of Enquiry (KLOE) introduced by the Care Quality Commission (CQC). By 31st March 2019, all health and social care organisations that provide NHS care through the NHS Standard Contract were required to provide NHS Digital with evidence of compliance with details of their position against the DSPT.

The NDG was pleased to see the toolkit redesigned in line with her recommendations and welcomed efforts to make it suitable for a wider range of organisations, particularly smaller social care organisations.

The cyber security team at NHS Digital has so far been involved in six CQC inspections of data security standards at NHS Trusts. A recent update to the NDG on its early findings has indicated that key areas of focus must be ensuring that trusts have suitably trained and qualified personnel within the field of information security, and that IT professionals in particular have more tailored security awareness training that looks beyond the basic competency level.

In a further development, the DHSC appointed Dame Fiona Caldicott to become the Independent Reviewer of decisions it will make under the Network and Information Systems (NIS) Regulations. These regulations place security and reporting requirements on operators of essential services in the health sector. They were designed to ensure that operators of essential IT services such as NHS trusts are maintaining high cyber security standards. Where operators do not comply with these requirements, regulatory action, including penalties of up to £17 million, can be taken. They have the right of appeal to an independent third party. As Independent Reviewer, Dame Fiona will hear any such appeals.

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

Priority 2. To support, as appropriate, putting the post of the NDG on a suitable statutory footing so that the work to provide advice to the health and social care system can continue.

As early as November 2014 the Secretary of State proposed putting the role of the NDG on a statutory footing. This was welcomed by the NDG and her Panel as an important signal to the public that they had a champion to speak on their behalf and to protect the security of their health and social care data.

Although the Secretary of State's proposal had cross-party backing, there was no suitable Government bill to which it could be attached. Instead, the Government gave its support to a private member's bill[21], tabled by Jo Churchill, MP for Bury St Edmunds.

Progress of the Bill

The Health and Social Care (National Data Guardian) Bill 2016-17 made good headway, but did not complete its legislative stages before Parliament was prorogued in preparation for the general election of June 2017. Jo Churchill was appointed as a Government whip after the election, but her bill was taken up by Peter Bone, MP for Wellingborough, and introduced into the House of Commons on 5th September 2017.

Private members' bills commonly fail to reach the statute book because they may founder at any stage in the House of Commons or House of Lords if they provoke dissent. In this case there was cross-party support for enhancing the authority of the NDG. The Bill passed through both Houses of Parliament without amendment and received Royal Assent on 20th December 2018[22].

The Secretary of State signed an order to provide for the commencement of the provisions of the Bill from 1st April 2019 and confirmed that Dame Fiona Caldicott would be the first holder of the office for an initial term of 18 months.

The Act's key elements

The Health and Social Care (National Data Guardian) Act 2018 contains five key elements:

1. To establish the statutory role of the National Data Guardian for Health and Social Care.

2. To give the NDG the power to publish formal guidance about the processing of health and adult social care data in England.

Such formal guidance may be directed to public bodies exercising functions within the health and adult social care sector in England (and private organisations which contract with them to deliver health services or adult social care). It imposes a corresponding duty on public bodies and providers within the health and adult social care sector to have regard to the NDG's formal published guidance.

3. To require the National Data Guardian to consult with appropriate persons before publishing formal guidance and to keep guidance under review.

4. To require the NDG to produce an annual report including a set of accounts, details of advice given, and guidance published in the previous financial year, and the priorities for the forthcoming year.

5. To give the NDG the power to provide informal advice, assistance and information to anyone in relation to the processing of health and adult

[21] https://www.parliament.uk/about/how/laws/bills/private-members/

[22] At 3rd reading in the House of Commons, Peter Bone graciously suggested that the legislation should become known as the Churchill Act.

social care data in England. Informal advice could be directed to any organisation or individual processing health and social care data. It would not result in any corresponding duty to have regard to the advice.

The NDG and her Panel regarded the enactment of these powers as a clear signal that Parliament understood the importance of maintaining public trust in the use of data. The theme of trust has always been at the centre of the NDG's work, with a focus on what can be done to help people to be aware of and more actively engaged in important decisions about how patient data is used and protected.

This view was confirmed in the 3rd reading debate in the House of Commons by Jackie Doyle-Price, Parliamentary Under-Secretary of State for Health and Social Care. She said: "I cannot emphasise enough the fact that the voice of the patient and the service user is really the paramount principle under which the National Data Guardian will operate, notwithstanding the fact that she will be working through the use of guidance to providers. It is basically taking the position of what is in the best interests of the patient. In so doing, we hope that the guidance she issues will establish confidence on the part of the public that their data is being used effectively."[23]

Working with regulators

It is clear from the Act that the NDG is not a regulator, but it is intended that she works with relevant regulators. Before gaining statutory authority the NDG was already working closely with the Information Commissioner and the Care Quality Commission. Refreshed Memoranda of Understanding (MoU) will confirm the continuing importance of these relationships now that the NDG's role has been placed on a statutory footing.

Children's social care data

During the passage of the Bill through Parliament the NDG and her team provided briefings for MPs and peers and discussed the contents of the Bill with a wide range of stakeholders. Two issues sparked particular interest. Firstly, it was noted that the NDG's remit covered data processed during the social care of adults, but not of children. The reason for drafting the Bill in this way was that the NDG will be accountable to the Secretary of State for Health and Social Care who has ministerial oversight of adult social care, while the social care of children comes under the authority of the Secretary of State for Education. There are different frameworks and lines of accountability for adult and children's social care. However, it is likely that issues may arise where children are receiving care from health services (inside the NDG's statutory remit) and social services (outside it), where data is flowing between services, or not flowing as it should.

An exchange of letters between the DHSC and the Department for Education (DfE) helped to establish a common view and eliminate the possibility of any difficulties around remit and responsibilities arising in the future. The two Departments agreed that once the Act came into force, "the NDG would be able to be consulted both formally and informally by the DfE and/or DHSC and, where appropriate, to raise issues with the DfE and/or DHSC, and to respond to consultations where it would be appropriate to share knowledge and offer advice from the adult social care arena and how this might relate to children's social care. It is considered that this interpretation is consistent with the NDG's power to give advice and information about the processing of adult health and social care data." Jackie Doyle-Price told the third reading debate in the House of

[23] 3rd reading debate columns 666-668. https://hansard.parliament.uk/Commons/2018-07-06/debates/0FEC92FF-4DF6-415E-A385-916EDCD2040D/HealthAndSocialCare(NationalDataGuardian)Bill

Commons that this "sensible interpretation … would not preclude the National Data Guardian from engaging constructively with the Department for Education on adult social care data and its interaction with children's social care data."[24]

Non-clinical demographic data and the NDG's remit

A second issue raised during Parliamentary debates was whether the definition of health and adult social care data that was being used to give the NDG her remit could be interpreted to exclude non-clinical demographic data such as a patient's home address and family details.

This possibility was of great concern to the National AIDS Trust, which feared that people's confidentiality could be eroded if their non-clinical demographic data was not to be afforded the same degree of protection as their clinical data. Polling undertaken by NHS Digital had found that the general public consider it as important that the NHS keeps their address confidential as their clinical information[25].

These fears were laid to rest by Lord O'Shaughnessy, Parliamentary Under-Secretary of State for Health and Social Care. In the third reading debate in the House of Lords, he said: "The Bill is drafted widely to allow the NDG to issue guidance about the processing of health and adult social care data. This should be interpreted broadly and would allow for the NDG to produce guidance on issues that impact on the processing of health and adult social care data. This would include, for example, good practice in security standards for storing health and adult social care data. This is an example of where guidance is not strictly focussed on health and social data itself, but about the processes and issues that could impact it. Almost anything that should be taken into account when processing health and adult social care data—or which broadly has the potential to impact, affect or influence that processing—would fall within the scope of that definition."[26]

Public consultation on the NDG's priorities

On 18th February 2019 the NDG launched a public consultation on how she should use the powers in the Act as the role moved on to a statutory footing starting 1st April 2019. The results of that consultation explaining her priorities for action are set out in *Section 3.*

[24] ibid
[25] https://digital.nhs.uk/news-and-events/latest-news/nhs-digital-statement-on-health-select-committees-report-into-patient-data-sharing
[26] https://hansard.parliament.uk/Commons/2018-07-06/debates/0FEC92FF-4DF6-415E-A385-916EDCD2040D/HealthAndSocialCare(NationalDataGuardian)Bill

Priority 3. To work alongside others to encourage proper sharing of data in genomic medicine and to contribute to the thinking about how patients should be engaged about this.

The fast-developing science of genomics is showing huge potential for providing more accurate diagnoses for patients, better and more individualised treatments and new opportunities for screening and prevention. On the one hand, genomic data may not be so different from other clinical information; on the other, the way in which genomic data, by its very nature, may need to be used puts confidentiality to the test. Whilst good clinical practice in genetics requires the sharing of familial information, what interests the NDG is the requirement for genomic and clinical data about individuals to be shared much more widely than might be expected.

For example, when a doctor or scientist gets a genetic test result for patient A, they won't necessarily know the significance of that result without examining information about many other individuals. That will allow them to see if anyone else has had the same result, and what their symptoms or other characteristics were, in order to help make a diagnosis or decision about treatment for patient A. This approach requires careful explaining to patients so that their trust is deservedly maintained.

The NDG and her Panel have enjoyed engaging with the genomics community at various events, including the Festival of Genomics in January 2019. They gave advice to the team from NHS England and Genomics England that prepared for the launch of the NHS Genomic Medicine Service (GMS) in October 2018. The service aims, in time, to provide about 750,000 genomic tests each year. A national network of hub laboratories will work collaboratively to provide a comprehensive national service for the NHS.

The NDG and her Panel met representatives from NHS England and Genomics England three times in 2018 to discuss the arrangements they were putting in place for patients to become adequately informed before undergoing genomic testing – and to give their consent.

The result was a decision to implement a double consent model. Patients are to be asked to give consent for testing for the purposes of their own direct care. And they are to be asked separately whether they consent for their genomic data to be used for research. Refusal to give consent for research will never prevent a patient from accepting the benefits that genomic testing can bring for their own direct care. The service is looking to give patients every reason to say "yes" to research, while ensuring that this is a free decision, with no impact on the clinical aspect of their genomic care.

In December 2018, the NDG wrote to Professor Dame Sue Hill, Chief Scientific Officer, NHS England, and Professor Mark Caulfield, Chief Scientist, Genomics England, welcoming the progress that had been made. She said: "We welcome the step forward marked by the launch of the GMS test directory in October. It brings us closer to the mainstreaming of genomics in the NHS and with it the exciting prospect of many more patients being able to access the more personalised medicine that genomics may offer … Your proposed consent model ensures transparency for patients about how their data may be used appropriately, and what choices they may make, while also allowing for clinical pathways to remain effective."

Genetics and insurance

Members of the NDG's Panel participated in the review of the Code of Genetic Testing and Insurance[27], published in October 2018, and gave advice to ensure clarity for patients about their rights in relation to genetic tests when they are seeking health insurance. The Code says that insurers will not require or pressure an applicant to undertake a predictive or diagnostic genetic test in order to obtain insurance. Applicants do not need to tell an insurer about any genomic testing that suggests a risk of future disease, unless they are applying for life insurance over £500,000 and have had a test for Huntington's Disease as part of their care.

[27] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751230/code-on-genetic-testing-and-insurance.pdf

Priority 4. To support work to maintain public trust in a confidential health service.

The NDG has consistently emphasised the importance of public trust. Her focus has been on what can be done to help people to understand and influence important decisions about how their data is used and protected. It is her view that no project, however worthy its aims, will succeed unless those in control of people's data act in a way that inspires and retains public trust. During 2018-19 the NDG intervened to maintain public trust in a confidential health service by giving advice that helped to resolve several difficult issues.

Use of NHS data to trace migrants

The first of these problems concerned arrangements for the Home Office to ask NHS Digital for information, derived from GP registration records, about the latest known address of people suspected of breaching immigration law. This issue had been causing concern since the Partridge Review in 2014[28] exposed how this tracing service had been working. An account of the NDG's early involvement in this issue was given in her progress report in December 2017.[29]

In January 2018 a Health and Social Care Committee inquiry into the disclosure of data to the Home Office included taking evidence from a member of the NDG's Panel. The NDG subsequently wrote to Dr Sarah Wollaston, the committee chair, saying: "At the core of my concerns is the impact that I believe this approach to disclosing confidential data may have on a matter of paramount importance – the maintenance of public trust in a confidential health service."

The request for data that doctors would consider to be confidential was justified on the basis that this action was in the public interest. Doctors' professional codes stipulated that confidential information may be disclosed in the public interest in relation to the detection, investigation or punishment of *serious* crime. When NHS Digital considered releases of names and address data to the police for law enforcement, it did indeed apply a serious crime threshold. However, it did *not* do so when it came to releases of such data for the purposes of immigration enforcement. The NDG had numerous concerns about the data sharing agreement that was set out in the Memorandum of Understanding (MoU) between the DHSC, NHS Digital and the Home Office. Her letter to Dr Wollaston, outlining these concerns, was published by the Committee in the evidence to this inquiry.[30]

In May 2018, the Government announced that the DHSC/NHS Digital/Home Office MoU would be revised to raise the bar for the release of demographic information to the Home Office. Margot James, Minister of State for Digital and the Creative Industries, told MPs during consideration of the Data Protection Bill [Lords] on 9th May 2018: "The bar for sharing data will now be set significantly higher. By sharing, I mean sharing between the Department of Health and Social Care, the Home Office and, in future, possibly other Departments. No longer will the names of over-stayers and illegal entrants be sought against health service records to find current address details. The data sharing, relying on powers under the Health and Social Care Act 2012, the National Health Service Act 2006 and the Health and Social Care Act

[28] https://www.gov.uk/government/publications/review-of-data-releases-made-by-the-nhs-information-centre
[29] https://www.gov.uk/government/publications/national-data-guardian-2017-report: pages 11-12
[30] https://publications.parliament.uk/pa/cm201719/cmselect/cmhealth/677/67712.htm#_idTextAnchor038

2008, will only be used to trace an individual who is being considered for deportation action having been investigated for, or convicted of, a serious criminal offence that results in a minimum sentence of at least 12 months in prison." [31]

The NDG welcomed the Government's rethink and confirmed that she will be pleased to review any revised MoU.

DeepMind and the Royal Free data sharing

Another issue that continued to attract the attention of the NDG was the use of confidential NHS patient data by DeepMind Health, a UK subsidiary of Google. As explained in the NDG's progress report in December 2017, the NDG liaised closely with the Information Commissioner's Office over the work DeepMind Health had done with the Royal Free London NHS Foundation Trust to develop and test an app, known as Streams, to track acute kidney injury. During the project the legal justification for using the personally identifiable data of 1.6 million current and former patients was that it might benefit their direct care. For that reason it was suggested that they might be presumed to have given implied consent to the sharing of their data with DeepMind Health. The Information Commissioner asked the NDG to give advice on the use of this common law legal basis. The NDG's view was that this legal basis was not appropriate; it would not match with patients' reasonable expectations about how their information might be used[32].

The Information Commissioner was also concerned, and in July 2017 found that the Royal Free had not complied with data protection law and that it should commit to changes, including an independent audit. The Royal Free commissioned Linklaters to carry out the audit, which was delivered in May 2018.[33]

The NDG and her panel considered the audit's findings and disagreed with some of its claims, in particular the position Linklaters had taken on confidentiality – namely, that the touchstone of whether there is a breach of confidence is to be judged from the point of view of the clinician, rather than the patient. She is firmly of the view that it is right to place the patient's perspective, not the professional viewpoint, at the centre of judgements about where confidential data may or may not be used.

The Information Commissioner acknowledges that the health and care sector needs further clarity in this area and will work with the NDG in order to ensure that data can be used to implement healthcare technologies lawfully and in ways that empower patients.

Another NHS organisation using DeepMind's Streams app is Imperial College Healthcare NHS Trust. During 2018 the Trust sought to engage with the NDG to ensure that this was done in compliance with the common law and the reasonable expectations of patients. Imperial instructed DeepMind to start processing current in-patients' test results shortly before their clinical go-live in January 2019. It gave the health and care professionals who were personally responsible for caring for those in-patients secure access from a mobile device to their patients' latest test results. The NDG thanked Imperial for their open engagement which had been helpful to her understanding of their careful work to implement this technology. This good outcome showed how cutting-edge technology can be introduced in line with Caldicott principles and without compromising public trust in a confidential health service.

[31] https://hansard.parliament.uk/commons/2018-05-09/debates/CE43B0ED-87D3-4F63-B8A4-2A66964790C2/DataProtectionBill(Lords) Column 757

[32] https://www.gov.uk/government/publications/request-for-correspondence-between-the-ndg-and-the-royal-free

[33] https://www.royalfree.nhs.uk/news-media/news/royal-free-london-publishes-audit-into-streams-app/

NHS Code of Practice on Confidentiality

The NHS Code of Practice on Confidentiality 2003 provides guidance to frontline professionals to ensure they know how to confidently use, protect and share patient information in the patients' best interest and so that patients' reasonable expectations about their privacy are met. The NDG has been contributing to the work of those who have been entrusted with the complex task of updating this Code. This work had not concluded by the end of 2018-19, but through membership of the Code's expert reference group a representative from the NDG's Panel will continue to take an interest in the rewriting of this key piece of guidance, providing help and feedback wherever appropriate.

Local Health and Care Record Programme

The Local Health and Care Record (LHCR) programme is supporting a range of regional collaborations of NHS organisations and local authority social care departments that are being formed to encourage information sharing to improve care and patient experience. Initially they will share information about patients and service users for direct care purposes within a LHCR region. Subsequently NHS England 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. As part of this programme, NHS England has taken advice from a steering group of stakeholders including a representative of the NDG's Panel about an information governance framework to help the LHCRs to comply with data law.

This work has raised some difficult questions: what is the legal basis for taking a shared record that is available for the purpose of direct care and de-identifying it for other purposes? Does de-identified data remain personal under GDPR? The NDG will do what she can to help to resolve these issues.

Use of data about cancer patients

Lord O'Shaughnessy, then Parliamentary Under-Secretary of State for Health and Social Care, asked the NDG to look into the release of data on nearly 180,000 lung cancer patients to a firm affiliated with tobacco companies. Public Health England sent the information to the US consulting firm William E. Wecker Associates under Freedom of Information (FOI) law. The data was anonymised, but PHE received much media criticism for supplying information to a company associated with the tobacco industry that had not been made publicly available.

On 25th June 2018, the NDG replied to Lord O'Shaughnessy saying that her Panel had looked into the matter. "We entirely accept that the process of considering requests under the FOI legislation must not take into account who is asking for the information or why they want it ... [However,] ... we believe that it would have been more conducive to building public trust if the information provided to William E. Wecker Associates had also been made generally available at the same time via publication. Publishing the information openly could have helped to reduce the suspicion that a commercial company had gained advantage from publicly-funded services in order to further its own interests - interests which, in this instance, appear diametrically opposed to those of the public and in particular to those of the patients whose data enabled the creation of the statistics."

The NDG also talked to PHE about its Review of Informed Choice for Cancer Registration (RICCR)[34], suggesting further action to ensure that patients are informed about the existence of

[34] https://www.gov.uk/government/publications/review-of-informed-choice-for-cancer-registration-ncras-response

the cancer registries and the use of the data from them.

PHE has been keeping the NDG informed of its progress in this area. It has developed a National Disease Registration Service Engagement and Awareness team to lead the response for the RICCR and to implement its recommendations.

Patient experience surveys

In a further development, ministers decided that the National Data Opt-out would not apply to the surveys that are run to measure patients' experience of GPs, secondary care, outpatients and cancer treatment. Cancer charities and some NHS officials had argued that applying it to the surveys would undermine their statistical validity and negatively impact care. Ministers decided that the National Data Opt-out would not apply.

Steve Brine, then Parliamentary Under Secretary of State for Public Health and Primary Care, announced that because improving cancer care is a priority in the NHS Long Term Plan, and because learning from the experiences of patients is crucial to shape services, the national patient experience survey would not be within scope of the opt-out.

Responding to the announcement, the NDG acknowledged the public interest in allowing individuals to be given the choice of taking part in these important NHS surveys while ensuring that it is clear to all patients when health and care information about them will be used and in what circumstances they can opt out.

Engaging with people and organisations

The NDG receives a steady flow of inquiries from members of the public. Often these relate to concerns about how information on themselves or family members is being used. Processes are in place to deal with correspondence, which may result in advice, signposting and the NDG contacting other organisations to raise concerns.

The NDG also engages with organisations that approach her to seek advice on their plans for sharing data. This is part of the NDG's work to encourage good practice across health and care.

Priority 5. To consider how the NDG can best support the use of data in new healthcare technologies in line with patient expectations and preferences.

The NDG has frequently been impressed by the altruistic attitude shown by members of the public who are broadly content for their health and care data to be used for the benefit of society, subject to appropriate safeguards. However, engagement with the public has consistently shown that, alongside this support, there is concern about which organisations can use patient data and for what purpose. As the NDG noted in her 2017 report[35]: "Some individuals are prepared for commercial companies to have access to data collected by publicly funded health and care services as long as this is controlled and there is a public benefit. Others take the view there should be never be a commercial gain involved in such data sharing."

Against this background of controversy, the NDG committed to give consideration to a proposal in Sir John Bell's report to the Government in 2017 *Industrial Strategy: Life Sciences*[36] for a regulatory and commercial framework. He wanted it to be capable of ensuring that the value of innovations, built for example on algorithms generated using health data, is properly recognised by the NHS.

The NDG engaged with the Government's Office for Life Sciences, which progressed the proposal and in December 2018 published the second Life Sciences Sector Deal[37]. It gave a commitment to create a central framework for realising the benefits of NHS data, underpinned by five principles. All five are important, but the NDG was particularly encouraged by two of them:

- Any commercial arrangements agreed by NHS organisations should be transparent, clearly communicated, and not undermine public trust and confidence either in the NHS or wider government data policies.
- Any commercial arrangements agreed by NHS organisations should fully adhere to all national level legal, privacy and security obligations, including in respect of the National Data Guardian's Data Security Standards.

The NDG and her Panel were also encouraged by the "tech vision" launched by Matt Hancock, the Secretary of State for Health and Social Care, in October 2018[38]. He outlined plans to introduce minimum technical standards that digital and IT systems in the NHS will have to meet in order to provide secure communication among health and care organisations, giving appropriate access to real-time data. This should improve the sharing of information among care providers - in line with Caldicott principles - and ensure that patients, service users and their carers do not have to repeat themselves. In particular the NDG was encouraged by the fact that building and maintaining public trust cited in the guiding principles section of the document and by an enhanced commitment to give patients online access to their own records. This was recommended

35 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668729/NDG_Progress_Report_FINAL_v1.1.pdf

36 https://www.gov.uk/government/publications/life-sciences-industrial-strategy

37 https://www.gov.uk/government/publications/life-sciences-sector-deal

38 https://www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care

by the Information Governance Review in 2013.

During 2018-19 the NDG Panel gave feedback to support the development of new DHSC guidance for the development of apps. The guidance, *Clinical Safety Guidance Governance and regulatory requirements for decision supporting and making software in the NHS and Adult Social Care*[39], was published by NHS Digital in January 2018. The NDG also advised on initial drafts of the new code of conduct for artificial intelligence (AI) systems and other data driven technologies used by the NHS[40] and met with DHSC officials to discuss the next steps for developing this.

[39] https://digital.nhs.uk/binaries/content/assets/legacy/word/f/p/clincal_safety_guidance1.docx
[40] https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology

Priority 6. To continue work to explore consensus about the way that patients' reasonable expectations should influence and shape the way that data is shared to support individuals' direct care.

In 2018 the NDG joined with Connected Health Cities to commission a citizens' jury to explore people's reasonable expectations. The question at issue was when members of the public would reasonably expect confidential information about their health and care to be disclosed by the professionals caring for them and when they would expect it to be kept private.

This question was of more than academic interest. During 2017 members of the NDG's Panel had become concerned about the way "implied consent" was increasingly being used as a legal basis under common law for sharing confidential information.

Relying on implied consent is often acceptable among members of the direct care team who have a legitimate relationship with the patient. For example, when a patient agrees to their GP referring them to a hospital consultant, the GP will normally work on the basis that the patient expects the referral to include information about them, their symptoms and other relevant details that the consultant may need to know to provide care. The GP will not normally seek specific permission to include confidential information in the referral. Thus consent to that is implied. However, implied consent cannot be used to justify more indiscriminate disclosure of a patient's confidential information, for example to researchers, administrators or direct care professionals who are not looking after that individual patient.

At two seminars in 2017[41] [42] the NDG explored whether the legal concept of "reasonable expectations" might provide an alternative way of supporting sharing. If patients and service users could reasonably expect their confidential health and care data to be shared in certain circumstances, that would have a bearing on their expectations of privacy. In circumstances where individuals had no reasonable expectation of privacy, there might be no need for explicit or implied consent. The lawyers, ethicists and health and care professionals who attended the seminars perceived challenges around some uses of implied consent as a legal basis for sharing data to support care. Many of those present indicated that they believed the legal concept of reasonable expectations might help to deal with those challenges.

To explore the idea further the NDG and Connected Health Cities commissioned Malcolm Oswald of Citizens' Juries CIC to run an exercise over three days in January 2018, when 17 people gathered at Friends' Meeting House in Manchester to test a number of NHS scenarios.[43] In each case, the participants were asked to judge whether it was reasonable for a patient to expect the information to be shared, or whether it was reasonable for the patient to expect privacy. Over

[41] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663089/Exploring_consensus_on_reasonable_expectations_-_July_2017_seminar_FINAL.pdf

[42] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742947/830_-_Supporting_health_and_care_professionals_to_share_data_in_line_with_patient_expectations_-_October_2017_seminar_FINAL.pdf

[43] https://www.connectedhealthcities.org/chc-hub/public-engagement/citizens-juries-chc/citizens-jury-2018/

the three days, the citizens heard from expert witnesses and worked in groups on the jury questions.

The 10 scenarios and questions were designed to try to replicate the reasonable expectation test that a court might apply when considering whether there had been a breach of common law. In other words, the jury was being asked to give a view on whether an average person of normal sensibilities would find such sharing reasonable in the circumstances.

The jury was asked to consider the uses of the data relating to a fictional patient we called Anita. Anita initially goes to the GP with an eye problem. The 10 scenarios follow her and her data through various parts of the health and care system and at each point the jury was asked whether Anita would have reasonably expected privacy or sharing. She was our "average person of normal sensibilities" and the jury was asked to consider the scenarios from her perspective.

It was interesting to note that a majority of the jury said data-sharing would be reasonably expected in all but one of the scenarios (where the GP encounters Anita's husband and discusses her case), although the numbers expecting sharing or privacy did vary across the scenarios.

During the process, the jurors naturally gravitated more to discussing whether the ends of the data sharing were desirable and if data sharing was necessary to achieve those ends. The facilitators, and the questions put to the jury, continued to emphasise "reasonable expectations", but it seemed that our jury was more interested in whether they supported the data sharing scenario rather than whether the data sharing could be reasonably expected.

This is arguably reflected in the list of reasons the jurors gave why data sharing might be reasonably expected. They were broadly focused on supporting outcomes (for the individual and for the health and care system and society more generally) that the jury would want to see - rather than on their expectations. Interestingly, the more that was explained to the jury, the more comfortable they became with certain uses of data. For example: when looking at data being used to help a company develop artificial intelligence software, there was some uncertainty; but when the uses and safeguards were explained, a majority were comfortable and supportive.

The NDG and Dr Mary Tully, Director of Public Engagement, Connected Health Cities, concluded that there is a dynamic element in defining people's reasonable expectations. In an article in August 2018[44] they said: "The provision of good information to patients and service users allows expectations to be informed. The more we provide transparent and well-designed communications about data usage, the more confident we can be of where reasonable expectations might lie. Where data is being used in novel or controversial ways, the need to provide information to patients and service users is likely to be higher. By placing the expectations of the patient at the centre of discussions about how confidential patient information may be used, by acting consistently according to well-understood professional norms, by listening to members of the public such as our jury about what they want to see and by communicating well so that people's expectations are informed, the health and care system (or indeed any data use initiative) will be taking steps to ensure that it is acting in a way that is trustworthy."

The National Data Guardian intends to progress the concept of reasonable expectations during 2019-20, and will aim to issue a plan outlining the next steps.

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

Priority 7. To continue to liaise with a range of government bodies to further NDG objectives, such as the safe and transparent use of data.

Probably the most significant development for those responsible for data during this period was the introduction of the EU General Data Protection Regulation (GDPR), which took effect on 25th May, 2018. It was incorporated into UK law by the Data Protection Act 2018 (DPA 2018). The NDG and her Panel liaised with various Government departments and other official bodies in the national GDPR working group and contributed to the advice on implications for the NHS, social care and partner organisations that was provided through the Information Governance Alliance.[45]

The DPA 2018 placed a positive emphasis on individual rights, strengthened organisations' duty of transparency and helpfully clarified statutory legal requirements for the processing of data. Section 171 of the Act[46] introduced a criminal offence for knowing or reckless re-identification of individuals; this had been recommended in the NDG's Review of Data Security, Consent and Opt-outs.

The NDG was also pleased to see safeguards in the DPA concerning the regulations which allow a Secretary of State to introduce new legal bases for processing data. The Act made clear that the Secretary of State would need to first consult the Information Commissioner and such other persons as he considers appropriate: an example would be where the regulations touch on healthcare matters and/or the processing of patient data. In such a case, the Secretary of State might consider it appropriate to consult, for example, the NDG, relevant healthcare bodies and relevant medical associations.

In spite of these positive developments, the introduction of GDPR and DPA 2018 contributed to some confusion across the health and care sector about the interplay between GDPR and the Common Law Duty of Confidence, and in particular the role of consent. This has not yet been fully resolved. Guidance such as that produced by the national GDPR working group has made it clear that, for GDPR/DPA 2018 purposes, clinicians and social care staff should *not* rely on the consent of their patients and service users as the legal basis for processing data. Instead they should seek other legal avenues that are available under Articles 6 and 9 of the GDPR.

However, explicit consent or implied consent will still usually be required to satisfy the Common Law Duty of Confidence. The NDG has heard that for frontline staff, the instruction that they must not use consent for GDPR purposes, but must use it for common law purposes, is causing confusion. Organisations can be fined for breaches of the GDPR/DPA 2018; and care professionals can be struck off for breaches of confidence, as defined in their professional codes. The NDG is seeking the support of other bodies to provide the necessary clarification.

Care Quality Commission

In July 2018 the Care Quality Commission published a review of how local health and social care systems in 20 areas were working together to support people aged 65 and over. Its report, *Beyond barriers: how older people move between*

[45] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance
[46] https://www.legislation.gov.uk/ukpga/2018/12/section/171

health and care in England[47], found that organisations:

- were prioritising their own goals over shared responsibility to provide person centred care;
- did not always share information with each other which meant they weren't able to make informed decisions about people's care;
- were not prioritising services which keep people well at home;
- planned their workforce in isolation to other services.

The NDG wrote in August 2018 to Ian Trenholm, the CQC chief executive, saying:

My advisory Panel and I … appreciated the opportunity to meet with CQC colleagues and discuss the report's findings and recommendations … We have been struck and saddened that many of the deficits in information sharing which we identified in The Information Governance Review: information to share or not to share[3] persist. As you may know, our concerns about a 'culture of anxiety' acting as a barrier to good data sharing in the best interests of the individual were what led us to introduce the seventh Caldicott Principle when we published that report in 2013. That principle states that 'the duty to share information can be as important as the duty to protect patient confidentiality'.

I support the recommendations outlined in the *Beyond Barriers* report and the focus on encouraging organisations to work in collaboration rather than focus narrowly on their individual remits and boundaries. I do hope that work in this area will continue and would be happy to discuss with you how my advisory panel and I might support it …"

Department of Work and Pensions review of consent for further evidence

During Autumn 2018, and in the light of GDPR, the Department for Work and Pensions (DWP) updated the wording of the statement it uses to collect consent from claimants when it needs to access their health information. This consent is collected by DWP on behalf of relevant health professionals. This consent then enables health data about that person to be disclosed to DWP by the health professional for the purposes of administering their benefit claim. The NDG was asked to review this statement, and provided comments on a number of iterations of the materials, ensuring that there was clarity for patients on the information that may be requested from their doctors and who will have access to it.

Centre for Data Ethics and Innovation

Dame Fiona welcomed the creation of Centre for Data Ethics and Innovation, which is an advisory body set up by Government to investigate and advise on how to maximise the benefits of data-enabled technologies, including artificial intelligence (AI).

The NDG response to the Centre's consultation on its activities and work agreed that it was highly important that data and AI should be used in a way which is ethical and supports innovation. We welcomed the commitment to working with other institutions and noted that in the field of health and care, there are mature and well understood systems of governance, custom and practice in relation to the use of data and that it would will be important for the Centre to understand these norms and take learning from other sectors where relevant. The NDG was pleased to receive a positive response and has enjoyed good engagement with the leadership of the Centre. Our organisations are planning to develop a memorandum to describe how we will

[47] https://www.cqc.org.uk/publications/themed-work/beyond-barriers-how-older-people-move-between-health-care-england

work successfully together in the best interests of the public.

Digital Economy Act

The DEA was a significant piece of legislation introduced in 2017, allowing for greater data sharing across government.

The NDG was consulted about the codes that underpin the use of these data sharing powers. She was pleased to note that health and adult social care bodies were not included in the scope of these powers[48]. The code includes a commitment that this would continue to be the case until the recommendations of the NDG Review were implemented and there had been public consultation, including with appropriate representative health bodies, adult health and social care bodies. The NDG is represented on the review board that considers the way the public service delivery powers are being used.

[48] https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice/code-of-practice-for-public-authorities-disclosing-information-under-chapters-1-3-and-4-public-service-delivery-debt-and-fraud-of-part-5-of-the-di

Priority 8. To encourage the improvement and development of training and education offered to health, care and information governance professionals to support safe and appropriate use and sharing of data.

In 2018-19 there was a strong impetus for improved training in the safe and appropriate use of health and care data, which came as a direct result of recommendations in the NDG's 2016 Review of Data Security, Consent and Opt-outs.

During the year all organisations with access to NHS patient data had to complete an online self-assessment to demonstrate that they could be trusted to maintain the confidentiality and security of personal information. One of the requirements was to show that staff were adequately trained in data security and appropriate information sharing, as evidenced by their ability to pass a mandatory online test.

By the end of March 2019 more than 30,000 organisations had registered with this new Data Security and Protection Toolkit (DSPT) and 26,800 organisations had published an assessment against the NDG's data security standards.

The NDG's 2016 Review had called for a redesigned Toolkit to embed her new data security standards and for annual role-appropriate training to be mandatory for all who work in health and social care. The DSPT replaced the existing Information Governance Toolkit and gave increased emphasis to cyber security and the benefits of appropriate information sharing.

Despite this being the first year of evidencing against a new, higher standard, the number of organisations completing an assessment was up 18% when compared with the predecessor IG Toolkit (by an additional 4,200 organisations). This will have a positive impact on data security across health and care. NHS Digital is currently analysing the returns made using the DSPT and intends to publish its initial findings later this year.

During 2018-19 the NDG and the UK Caldicott Guardian Council (UKCGC) worked with NHS Digital's DSPT team to ensure that the Caldicott Principles were adequately reflected in training materials, with due regard paid to the importance of information sharing among those directly responsible for an individual's care. A specific question was added into the staff awareness questions to cover the balance between confidentiality and sharing information for care.

Organisations were encouraged to use the national e-learning for health (ELfH) data security training tool. The UKCGC engaged with the ELfH to ensure support for information sharing.

The UKCGC does not itself provide training, but it does offer Caldicott Guardians vital peer-to-peer support, and helps those who perform the Caldicott Guardian function within their organisations to resolve complex questions about the balance between confidentiality and information sharing, involving ethical as well as legal issues. For example, the UKCGC worked with the police to clarify when it may be appropriate for Caldicott Guardians to make information available to help trace a missing person. Although protecting medical confidentiality is a fundamental safeguard, there are circumstances when sharing information to safeguard the victims of crime or abuse is ethically the right thing to do. The UKCGC and the National Crime Agency's Missing

Persons Unit[49] have published formal guidance[50] outlining good practice considerations including the sort of information the police should provide upfront when requesting information from NHS organisations and GPs.

Other examples of UKCGC broader educational work included regional workshops at which the Caldicott Guardians from a wide range of health and care organisations meet to learn from each other's experience.

The NDG has liaised with the Academy of Medical Royal Colleges, which sets standards for the way doctors are educated, trained and monitored across the UK. It has engaged with the Topol Review, led by cardiologist, geneticist, and digital medicine researcher Dr Eric Topol, which explores how to prepare the healthcare workforce, through education and training, to make the most of innovative technologies.

During 2018-19 the NDG and UKCGC met with the Faculty of Clinical Informatics, which has been established as a UK professional membership body for all clinical informaticians, including health and social care professionals. Its vision is for safe, effective and efficient healthcare through the best use of information and information technology. Key objectives for the Faculty up to 2020 include: establishing clinical informatics as a recognised profession, developing professional standards, providing training and accreditation for individuals and courses, and supporting recruitment and careers in clinical informatics. The Faculty's prime aim is to assist in meeting the demand for increasing numbers of well-trained clinical informaticians able to work with others to deliver their vision.

The NDG has also had continued engagement with the NHS Digital Academy, a virtual organisation set up to develop a new generation of excellent digital leaders who can drive the information and technology transformation of the NHS. The NHS Digital Academy is delivered in partnership by a consortium comprised of Imperial College London, the University of Edinburgh and Harvard Medical School. The NDG has monitored and reviewed progress of the first cohort of graduates to complete the year-long learning programme and earn a post-graduate diploma in digital health leadership. This has also provided the opportunity to input into the syllabus.

The NDG has maintained regular representation on the Data and Cyber Security Programme Board. This has recently included supporting NHS Digital and the National Cyber Security Centre working together rapidly to upgrade the DSPT to integrate the most appropriate elements of Cyber Essentials Plus (CE+), including accreditation.

[49] https://missingpersons.police.uk/en-gb/home

[50] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/802433/Information_sharing_between_police_and_health_and_care.pdf

Section 3. Looking forward: NDG's new priorities

Dame Fiona and her panel decided that the NDG's move to a statutory footing presented a good opportunity to consult about what her key priorities should be.

A public consultation ran from the 18th February to the 22nd March 2019, proposing four broad priorities for the NDG and potential focused areas of interest within each of these. The consultation document made clear that the NDG could not deliver these priorities alone. It also explained that the proposed priorities would require ongoing work in the coming years for many organisations working together.

It also set out that these would not to be the only things the NDG would do. She would also 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.

Respondents were invited to comment on the four proposed priorities, to tell whether they agreed that they should be prioritised or not and to make alternative suggestions.

We received 118 responses to our consultation, around from organisations, half from individuals. All responses were carefully reviewed and assessed.

Our consultation response document[51] provides a summary of the feedback we received and outlines how we took this into account to refine our proposals to three priorities which the NDG will pursue as the role moves onto a statutory footing:

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).

[51][51] https://www.gov.uk/government/consultations/national-data-guardian-a-consultation-on-priorities

- 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.

Section 4. Financial statement
March 2018-April 2019

Total income

£500,000 (including VAT)

Total expenditure

£482,752.08 (including VAT)

Breakdown of expenditure

The Office of the National Data Guardian, provided by NHS Digital

£358,841.96 (including VAT)

Staff costs - £232,367.77

The Office of the 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
Communications Manager	8a
Business Support Manager	6

Non-staff Costs – £39,482.03

Non-staff costs include:

- Public engagement
- Communications
- Training
- Meeting rooms
- Travel and expenses

Overhead costs (central functions ICT, HR, Finance, utilities) - £27,185.16

VAT costs - £59,806.99

National Data Guardian panel / UK Caldicott Guardian Council member fees and expenses processed by Department of Health and Social Care - £123,910.00

This sum includes fees and expenses for members of the National Data Guardian's Panel and Steering Group, the UK Caldicott Guardian Council and the salary for the chair of the UK Caldicott Guardian Council.

Section 5. Appendices

Appendix A
The Caldicott Principles

1. **Justify the purpose(s)**

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

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

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

3. **Use the minimum necessary personal confidential data**

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

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

   Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. **Everyone with access to personal confidential data should be aware of their responsibilities**

   Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Comply with the law**

   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality.**

   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix B
Panel member biographies

Dr Joanne Bailey

Dr Bailey worked as a GP from 1989 until 2016 and gained a master's degree in healthcare ethics in 2002. Joanne is a Founding Fellow of and Appraisal and Revalidation Lead for the Faculty of Clinical Informatics. She is also a clinical ethics and law tutor at Cambridge School of Clinical Medicine and a First-tier Tribunal Member (Social Entitlement Chamber). In the recent past she was a member of NHS Digital's Independent Group Advising on Release of Data (IGARD) and previously chaired the Joint GP IT Committee of the British Medical Association and the Royal College of General Practitioners, and the Data Access Advisory Group at NHS Digital.

John Carvel

John Carvel is a journalist by profession and was a writer and editor at The Guardian for 36 years. He supported Dame Fiona Caldicott during the Information Governance Review[52], which was published in 2013. John is a non-executive director at Dorset Healthcare University NHS Foundation Trust and has in the past been a member of the Healthwatch England National Committee, deputy chair of the Care Quality Commission's National Information Governance Committee and a member of the Department of Health's National Leadership Council.

Mark Golledge

Mark Golledge is a programme manager at the Local Government Association (LGA), with responsibility for leading work on digital and data across social care and health. Mark's background is in information and technology areas across both Local Government and Health. In his current role Mark works closely with councils and represents the LGA on the National Information Board and has also worked closely with NHS England supporting health and care integration and new care models.

Dr Alan Hassey

Dr Alan Hassey was a GP in Skipton, North Yorkshire for 31 years, until retiring from general practice in June 2013. He is a member of the Royal College of General Practitioners (RCGP) Health Informatics Group (HIG) and has previously chaired both the HIG and the Joint GP IT Committee of the British Medical Association and RCGP. Alan retired from NHS Digital at the end of 2017, where he was the IG Clinical Lead & Deputy Caldicott Guardian. Alan became a Founding Fellow of the new UK Faculty of Clinical Informatics in 2017.

Rakesh Marwaha

Rakesh Marwaha is managing director of RM Innovations and Leadership, providing freelance consultancy in leadership, innovation and management for health and care. Before this, Rakesh was CEO of NHS Erewash Clinical Commissioning Group and delivered a successful new care model – the

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

multispeciality community provider vanguard. Rakesh has over 20 years senior experience in health and care commissioning and chaired the Derbyshire multi organisation Informatics, Technology and Governance Board for eight years, with CEO leadership on programme delivery and the Local Digital Roadmap.

Eileen Phillips

Eileen Phillips is a freelance writer and communications consultant. For the past 10 years she has developed a commitment to the responsible use of health and social care data and believes that transparent engagement with the public to build trust is the only route to securing the benefits from large scale data. Her past communications roles include head of media relations for the NHS IT Programme and head of media and public affairs at NHS Digital.

Professor Martin Severs

Professor Severs has more than 20 years' experience in senior clinical, academic and health informatics roles. He has recently retired (February 2019) from being the medical director and Caldicott Guardian for NHS Digital and prior to that was a consultant geriatrician and professor of health care for older people in Portsmouth. He was the clinical lead for Dame Fiona Caldicott's Information Governance Review in 2013. He chaired the Information Standards Board for Health and Care in England from 1999 until 2014, and has held numerous roles within NHS research, development and leadership, including leading on health information within the Royal College of Physicians and chairing the information advisory structure of the Academy of Medical Royal Colleges.

Anne Stebbing

Anne Stebbing is a consultant surgeon at Hampshire Hospitals NHS Foundation Trust, with a special interest in breast, and minor paediatric surgery. She is also a non-executive director for South Central Ambulance Service NHS Foundation Trust. Previously she has been the secondary care representative for East Berkshire Clinical Commissioning Group. Anne has a keen interest in the best use of technology in medicine, patient safety, and improving communication and until recently was Caldicott Guardian for her acute trust.

David Watts

David Watts is the director of adult services for the City of Wolverhampton Council and co-lead of the National Association of Directors of Adult Services (ADASS) Standards, Performance and Informatics (SPI) workstream. David maintains his professional registration as a social worker and is both an experienced practitioner and manager in adult social care. As co-lead of the ADASS national SPI workstream he takes a lead for the standards and governance theme. He also represents ADASS on the Professional Records Standards Board and National Data Opt-Out Programme.

Dr James Wilson

Dr James Wilson is a senior lecturer in the Department of Philosophy at University College London. At UCL he is also co-director of the Health Humanities Centre and Vice Dean for the Faculty of Arts and Humanities. His main research and teaching areas are public health ethics and the ownership

and governance of ideas and information. He is associate editor of the journal Public Health Ethics[53].

[53] http://phe.oxfordjournals.org/

Appendix C
NDG Panel Terms of Reference

Background

Dame Fiona Caldicott was appointed as the first National Data Guardian for health and care in England by the Secretary of State for Health, Jeremy Hunt, in November 2014. The NDG's role is to help to ensure that the public can trust their confidential information is securely safeguarded, that it is used to support citizens' care and achieve better outcomes from health and care services by advising and challenging the health and care system.

Dame Fiona Caldicott has said that she is guided by 3 main principles:

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

Aims of the panel

The NDG's panel was formed to support the NDG through the provision of expert advice to enable the delivery of the NDG's objectives and work plan.

Recognising the independence of the NDG, members of the panel will operate in an independent and transparent manner when advising the NDG and when undertaking work on behalf of the NDG. Members will not be expected to represent any organisations by which they are employed.

The panel will comply with the Standards in Public Life54 (also known as the "Nolan Principles). Members will be expected to declare any conflict of interests and abide by their terms of appointment and code of conduct at all times. Panel members will be remunerated in line with their terms of appointment.

Accountability

The National Data Guardian is accountable to the Secretary of State for Health. The panel is accountable to the National Data Guardian.

Membership

Membership of the panel will be by invitation from the NDG. The duration of appointment will normally be three years, and may be extended by a further three years. However, recognising the long-term nature of some of the matters on which the NDG is asked to advise, the NDG may choose to retain members with particular knowledge and experience beyond the normal duration of appointment.

[54] https://www.gov.uk/government/publications/the-7-principles-of-public-life

The constitution of the panel will generally range between twelve and sixteen members. The number will flex depending on the need and availability of particular expertise, and the work that the NDG is commissioned to undertake.

Members of the Office of the National Data Guardian attend panel meetings but are not members of the panel. Office members attend to ensure the smooth running of panel meetings, to provide input from an operational perspective and to follow up actions and agreed decisions made at panel meetings.

A list of the membership of the panel will be published and kept up to date on the NDG's web pages.

The UK Caldicott Guardian Council (UKCGC) is a sub-group of the NDG's panel.

The Chair of the UKCGC is invited to attend meetings of the panel as an observer.

Additional observers may be invited to panel meetings from time to time, by invitation from the chair for the whole or part of any meeting.

Meetings

Meetings of the NDG's panel will be chaired by the NDG or a nominated deputy.

There will generally be six meetings of the panel each year. Additional meetings, either of the full membership or a sub-group, will be arranged on an ad-hoc basis as required. Meetings will be arranged and supported by the Office of the National Data Guardian.

Minutes of the panel meetings will be published on the NDG website after approval at the following meeting.

Engagement and key relationships

The panel will advise the NDG on how to ensure that the public and patients' viewpoint is included in NDG work. In doing so the panel will not seek to replicate the responsibility of other organisations to consult or inform the public and will advise on how the NDG can work alongside other organisations where possible.

The work of the panel involves maintaining a number of key relationships including with the Department of Health, arm's length bodies, regulators, professional bodies and patient advocacy groups.

Steering group

In order to provide more regular support to the NDG in between panel meetings, a smaller group made up in the main of nominated panel members, take part in steering group meetings.

Membership of the steering group is by invitation from the NDG. The steering group will meet on a monthly basis.

Key tasks are undertaking initial reviews of issues and papers which might be considered by the panel, providing a space for more detailed consideration of some matters and providing guidance to the office on operational matters which require oversight.

An output of agreed actions or decisions from the steering group meeting will be shared with the panel on a monthly basis.

Appendix D

Events and speaking opportunities attended

Event / opportunity	Date	Speaker
Enabling better cancer care: data and intelligence for Cancer Alliances (roundtable)	17/01/2018	Dr Anne Stebbing
Artificial Intelligence and Health roundtable with Lord O'Shaugnessy, Parliamentary Under-Secretary of State for Health	28/02/2018	Dr James Wilson
Health data summit: National Voices and Understanding Patient Data event (presentation)	27/02/2018	Dr Joanne Bailey
Masterclass in healthcare ethics and law - Royal College of Surgeons in Ireland in Dublin. Presentation: Sharing of patient information: expectations and patient confidentiality	09/03/2018	Dame Fiona Caldicott
Medicine and Machines series: The Regulatory Algorithm Hacked workshop	19/04/2018	Dr Alan Hassey
DAC Beachcroft event presentation: What next for patient data? Is your organisation ready for 2018?	01/04/2018	Dame Fiona Caldicott
British Heart Foundation Summit 2018 presentation: Building public trust for the use of data	08/05/2018	Dame Fiona Caldicott
Caldicott Guardian Annual Conference	14/05/2018	Dr Joanne Bailey
Royal College of General Practitioners National Data Opt-out engagement event presentation: the national opt-out and what it means for public trust	24/05/2018	Dame Fiona Caldicott
Medicine and Machines series: Big Data, Digital Technologies & Healthcare workshop	18/07/2018	Dr Joanne Bailey
NHS England's 'Winter and Beyond' roundtable event	09/08/2018	Dame Fiona Caldicott
Topol Review: A roundtable discussion as part of the Topol Review, on preparing the workforce to deliver the digital future.	20/08/2018	Anne Stebbing

NHS Innovation Expo 2018 panel: Your Data Matters - trust and transparency in an age of digital transformation	05/09/2018	Dr Alan Hassey
Healthcare and data: How do we get it right? The Wellcome Trust and Understanding Patient Data	13/09/2018	Dame Fiona Caldicott
Genomics England's public dialogue on genomic medicine: stakeholder workshop	13/09/2018	Dr Joanne Bailey
UK Health Show Cyber Security Symposium presentation on the role of the opt-out and national data security standards in building public trust	25/09/2018	Dame Fiona Caldicott
Festival of Genomics presentation: Data Security and Enabling the Power of Genomics	24/01/2019	Dame Fiona Caldicott
British Transplantation Society Annual Conference presentation: Communicating Patient Information Safely	06/03/2019	Dame Fiona Caldicott
National Data Guardian event: Celebrating, reflecting, looking ahead	11/03/2019	Dame Fiona Caldicott
NHS Research and Development Forum: in conversation with Professor Sir Jonathan Montgomery	13/05/2019	Dame Fiona Caldicott
Dame Fiona Caldicott address to students at the University of Buckingham	22/05/2019	Dame Fiona Caldicott

Appendix E
Boards and groups NDG panel / ONDG staff attend (or have attended)

Dr Joanne Bailey

NHS Confidentiality Code of Practice Reference Group
NHS England Data Use Sub-group

Dr Chris Bunch

Data and Cyber Security Programme Board
Chair of the UK Council for Caldicott Guardians

Dame Fiona Caldicott

Lord O'Shaugnessy's Data Strategy Board (board no longer active)
Data Security Assurance Board

John Carvel

National Data Opt-out Programme Advisory Board *(board no longer active)*
Local Health and Care Record Information Governance Steering Group

Dr Alan Hassey

GDPR working group
GP Dataset for Secondary Uses Programme Board
Data Security Leadership Board

Ross Thornton (Office of the National Data Guardian)

Data Security and Protection Toolkit Steering Group *(group no longer active)*

Dr James Wilson

Research Advisory Group
Oversight Group for Deliberative Engagement on NHS data

Jenny Westaway (Office of the National Data Guardian)

National Data Collaborative for Health and Care
NHS England Data Use Sub-group
Information Governance Alliance Programme Board *(board no longer active)*
Digital Economy Act Public Service Delivery Review Board