

National Data Guardian for Health and Care 2017 report: Impact and influence for patients and service users

Published 12 December 2017

Contents

Foreword by Dame Fiona Caldicott	3
Background to the role of the National Data Guardian	6
Encouraging sharing of information in the interests of care	7
No ‘surprises’ and choice for the citizen	9
Dialogue with the public	12
Working with others	14
Independence	16
Looking ahead	17

Foreword by Dame Fiona Caldicott



Since my appointment as the National Data Guardian (NDG) for Health and Care in November 2014¹, I have made the focus of my role the need for more to be done to help people be aware and more actively engaged in important decisions about how patient data¹ is used and protected.

These are issues that matter to us all. The confidential information we share with doctors, nurses and social workers is vital for our Individual care. If treated carefully, legally and with public support, it can also help us to improve health, care and services through research and planning.

It is true that the discussions about data can be complex. To many people the technical considerations and legal frameworks may seem remote and the discussions can appear to take place in committee rooms amidst policy considerations which all of us find overly complex. But every policy question, each new initiative on which I have advised, has reinforced a fundamental requirement: the public must be included in understanding and supporting innovation which relies on data generated by their use of health and care services.

There is enormous potential for good in the use of patient data, whether for developing break-through treatments or for helping regulators identifying when things are going wrong. The NHS has an unrivalled data set that can be used to develop sophisticated tools to improve health, such as those being created in the field of machine learning. But progress must take place in a transparent way and people must be allowed to disagree with the use of their confidential information for research, service support and other purposes not connected to their individual care. Only on a basis of transparency and choice can trust be built. It has been demonstrated regularly and repeatedly that no project, however worthy its aims will succeed, unless those holding, sharing and using data act in a way that inspires and retains public trust.

I approach these matters not only as someone with expertise in these issues but also as a member of the public who uses these services. Keeping that point of view in mind, understanding the real distress caused by any breach of confidentiality and grasping how easy it is to lose peoples' confidence - are all necessary if I am to meet the responsibilities of being the NDG.

It is three years since I was appointed as the first National Data Guardian for Health and Care. Last month I accepted a request from the Secretary of State for Health to continue in the role for an interim period of two years as a Bill is taken through Parliament to place the role on a statutory footing. I am pleased that the Government has committed to making the NDG role a statutory one and I anticipate this happening during this Parliament. This therefore is an important moment to present the work that the role has addressed so far, which issues are currently priorities and how far my involvement has ensured that the patients' point of view has been understood, acknowledged and responded to. Once the role of the NDG is on a statutory footing, this report will become an annual one.

So, this report looks back over the period of my work as NDG. A significant part of the workload, reflected in this report, has been the Review of Data Security, Consent and Opt-outs, which was commissioned by the Secretary of State in September 2015, delivered in

February 2016 and published in July 2016¹. The Government response to that report was published in July 2017² and accepted all the recommendations in full. The implementation of these recommendations is crucial to ensuring public support for the use of health and care data to improve care and treatment.

As technology plays a greater role in supporting and enabling care, it can help us deliver better, more compassionate, efficient treatments and services for ourselves, our families, our friends, our neighbours - for everyone in society. But it is also the case that keeping data secure becomes both more important and more difficult to achieve as devices and electronic systems multiply. Public trust relies on knowing we can manage that data to the highest possible standards of security.

The WannaCry ransomware attack of May 2017, which affected a number of organisations, including NHS bodies, demonstrated that the cyber threat is real. The new data security standards set out in the NDG Review were designed to encourage and support leaders across the system to take the right steps to secure patient data.

We also need to offer the public a genuine choice. The opt-out provides the means to demonstrate to the public that their wishes are respected, and their concerns are understood and listened to. There should be no watering down of that option. We need to build trust carefully if the true benefits of sharing information are to be realised.

Other important areas of work have been considering new issues raised by developments in genomic medicine, questions about the sharing of health data across government, and advising on the use of data to support new technologies.

After my appointment as NDG, I committed to three guiding principles:³

The three principles:

1. To encourage sharing of information in the interests of providing direct care to an individual.
2. There should be no surprises to citizens and they should have choice about the use of their data.
3. There must be dialogue with the public, helping to increase their knowledge and choices about how data is used to improve health and care.

This report explores how these three areas - sharing information in the interests of care, ensuring no surprises and choice for the citizen, and encouraging dialogue with the public - still stand and matter more than ever. It shows they are necessary to building public trust, particularly as we live through a huge expansion in data generation and gathering and increased vulnerability to cyber crime.

For the NDG to have any effect for patients, there are two crucial factors - working in partnership with others and retaining independence. In view of the importance of these, in addition to the sections of the report which revisit the three guiding principles, there are two further thematic sections examining how partnership and independence have been pursued vigorously. It has ensured that our work has breadth, impact and influence.

¹ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

² <https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care>

³ <https://www.gov.uk/government/speeches/national-data-building-trust-across-health-and-social-care>

I carry out this role with the support of a panel of advisors for whose wise counsel I am immensely grateful. Their contribution is invaluable whether this is given through expertise and sound advice offered on the subjects we consider, by representing me at more events and meetings than I could ever attend alone or by supporting me in communicating our work through the preparation of reports such as this.

The panel shares with me a sense that the public conversation over how best to use health and care data has started. Our work now is to ensure this dialogue is sustained in an open and inclusive manner. Without such action it is unlikely that we will be able to derive maximum benefit for patients from the latest advances in data technology.

**Dame Fiona Caldicott MA FRCP FRCPsych
National Data Guardian for Health and Care**

Background to the role of the National Data Guardian

The NDG for Health and Care was appointed by Secretary of State for Health in 2014 and a consultation was undertaken during the autumn of 2015 about the role and functions the NDG should have⁴.

A foundation for this work was the Information Governance Review⁵ carried out for the Department of Health by Dame Fiona Caldicott, 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 1997⁶.

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 2015⁷.

This 2017 report takes up the story from then to maintain continuity and transparency.

The NDG is supported by a small team of officials and a panel of independent advisers. Although the work of the NDG is similar to that of IIGOP, the remit is broader and involves providing scrutiny, challenge and advice to Ministers, the Department of Health, the Department's arm's length bodies, and more broadly the health and care system - always acting from the viewpoint of the patient and wider public and as a champion of their interests.

The Panel acts under the direction of the NDG, who is empowered to work without invitation or constraint. Its terms of reference⁸ and membership⁹ are also made available on the NDG webpages.

A résumé of activity during this period can be found in the minutes of the NDG Panel, available on the NDG webpages¹⁰.

⁴ <https://www.gov.uk/government/consultations/the-role-of-the-national-data-guardian-for-health-and-social-care>

⁵ http://webarchive.nationalarchives.gov.uk/20130124064947/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digital_assets/@dh/@en/documents/digitalasset/dh_4068404.pdf

⁶ <https://www.gov.uk/government/publications/the-information-governance-review>

⁷ <https://www.gov.uk/government/publications/iigop-annual-report-2014>

⁸ <https://www.gov.uk/government/organisations/national-data-guardian/about/terms-of-reference>

⁹ <https://www.gov.uk/government/organisations/national-data-guardian/about#who-we-are>

¹⁰ <https://www.gov.uk/government/publications/national-data-guardian-panel-meeting-minutes-2017>

Encouraging sharing of information in the interests of care

The first of the principles outlined by Dame Fiona Caldicott, when she was appointed as NDG, was:

The first principle:

There is a responsibility on clinicians and other members of the care team to share information that directly affects the care of the person they are treating or supporting. Patients and service users expect this, and my interventions will focus on supporting and reinforcing this approach. The direct benefits such sharing can bring to people, by providing joined-up care, better diagnosis and treatment, are unquestionable.

This followed on from a key recommendation of the 2013 Information Governance Review (IGR)¹¹. It encouraged the use of information sharing in the interests of the care of an individual. In the IGR Dame Fiona added an additional principle to the existing six Caldicott Principles, which had been in place since 1997¹²: ‘The duty to share information can be as important the duty to protect confidentiality.’

This aimed to address the nervousness that health and care professionals demonstrated about sharing data, often citing concerns about breaking patient confidentiality. Together with anxiety about potential fines from the Information Commissioner, the IGR found these concerns were significant barriers to the joining up of information and the improvements in patient care and experience that this could bring. It remains the case that there is more work to be done to ensure that the seventh Caldicott Principle is properly understood and implemented.

The subsequent NDG Review of Data Security, Consent and Opt-outs, commissioned by the Secretary of State in September 2015, again underlined the importance of sharing information to support care. It provided evidence that patients usually expect far more sharing of health and care information occurs than often takes place.

The NDG Review found that many people assume that relevant medical facts about them, which are known to their GP, will be available to their hospital doctor. And that their hospital doctor, in turn will be able to access notes from a different NHS trust or service. Similarly, most patients would also expect that if they were, for example, discharged from hospital to recover in a care home, that the hospital would be able to ensure that information would be passed efficiently and appropriately to staff at the home so the transfer could be as seamless as possible. Similarly when referred for further treatment to a physiotherapist or counsellor, patients assume that their relevant medical history would be available as part of that new consultation. Sadly all too often these expectations are not met; instead, medical record systems operate separately and the relaying of relevant information relies on the patient themselves.

However, a number of local initiatives were commended in the NDG Review for vigorously pursuing better integration of health and care information. These range in scale and complexity, but all aim to put the focus on the patient and service user, building systems

¹¹ <https://www.gov.uk/government/publications/the-information-governance-review>

¹² The six Caldicott principles, applying to the handling of patient-identifiable information, are: justify the purpose(s) of every proposed use or transfer; don't use it unless it is absolutely necessary, and use the minimum necessary; access to it should be on a strict need-to-know basis; everyone with access to it should be aware of their responsibilities; and understand and comply with the law.

that exchange information securely in order to provide better care. Since the publication of the NDG Review there has been further encouraging growth in such schemes.

For instance, the NDG Review highlighted the Leeds Care Record, which benefits patients by enabling healthcare professionals treating them to log on and directly access relevant health information from GPs and hospitals. Patients have been directly involved in defining what data is made available. Since the publication of the NDG Review, the scheme has extended to include community, mental health and adult social care information in the record. This is just one example of the schemes being developed around the country.

The NDG and her panel have also looked at the sharing of data to support genomic and genetic clinical services. This project originated in some professionals working in this field raising concerns that variation in the approaches to information sharing was barring them from providing the most accurate diagnoses and treatment.

The NDG worked with the PHG Foundation and the Association for Clinical Genetic Science to hold an evidence session dedicated to this topic in October 2016. Clinical genetics professionals and clinical scientists present at the session explained why patient data needs to be shared for clinical genetics and genomics services to deliver the best possible care. This is because appropriate diagnosis may depend on an iterative process, which requires data from more than one individual, potentially across a wide geographic area, or even from across the world. There are blurred lines in the field of genomics between data use for individual care and its use to support care of others and research, which challenges conventional understandings of medical confidentiality.

In August 2017 the NDG published a paper¹³ which proposes two next steps to progress confidence in the sharing of data to support NHS clinical genetics and genomics services. Firstly, that more should be done to explore what information might be needed for patients to give valid consent to the use of data for their own individual care and to be used more broadly, including for research purposes. Secondly, that a project to reconfigure NHS genetic laboratories should conduct a Privacy Impact Assessment to examine the privacy implications of services sharing data. Both recommendations require an understanding of what are ‘reasonable expectations’ for a patient and how these expectations can be appropriately informed.

The NDG and her panel have also undertaken work to look at the area of ‘implied consent’, after hearing that professionals continue to experience uncertainty about how far this legal basis should extend. Implied consent is a legal basis in common law. It is relied upon by health and care professionals every day to ensure good care is informed by the right information about an individual (although it should be noted that in social care settings it is common for people to be asked explicitly about what information may be shared). For example, when a patient agrees to their GP referring them to a hospital consultant, she will normally work on the basis that the patient expects that the referral will include information about them, their symptoms and other relevant details that the consultant may need to provide care. The GP will not normally seek specific permission to include confidential information in the referral, thus consent to that is implied.

And yet the NDG has heard from professionals who are unsure about how far the legal basis of implied consent should extend. In response, the NDG panel published an article in

¹³ <https://www.gov.uk/government/publications/developing-a-consensus-on-data-sharing-to-support-nhs-clinical-genetics-and-genomics-services>

December 2016¹⁴ inviting debate about the issue - the feedback showing a wide range of views about how implied consent should work and an appetite for more guidance.

The NDG initiated a project to examine the circumstances under which data may be legitimately shared, and the role that a patient's 'reasonable expectations' play in shaping these circumstances. A seminar to examine this question took place in July 2017 in conjunction with the University of Sheffield's Sheffield Solutions¹⁵. It brought together an invited audience of clinicians, legal experts, ethicists and other experts in information sharing. The seminar reached a tentative conclusion that further exploration from a legal, clinical and patient perspective should be given to the legal concept of 'reasonable expectations' to assess its potential to extend the circumstances under which disclosure is lawful.

In October 2017, a second seminar in conjunction with Sheffield Solutions examined the concept more closely with frontline health and care professionals. The health and care professionals present perceived challenges around some uses of implied consent as a legal basis for sharing data to support care and many of those present indicated that they believed the legal concept of reasonable expectations might help with these challenges.

Reports of both these events have been published¹⁶ and the next stage of this work will be a piece of public engagement in the new year to involve a citizens' jury (where a cross-section of the public hear from witnesses, deliberate together and reach reasoned conclusions) and public survey to examine what members of the public would expect in relation to the sharing of their information to support their individual care. This work is being carried out in partnership with Connected Health Cities¹⁷ and Citizens Juries CIC¹⁸.

No 'surprises' and choice for the citizen

The second principle outlined by Dame Fiona on her appointment as NDG was:

The second principle:

Second, there must be no surprises to the citizen about how their health and care data is being used. This is a complex arena where the public benefits of access to big data, gathered from the millions of health and care activities occurring daily, need to be balanced with the public's right to know and, if they wish, object. Failing to offer this choice to people can accelerate discontent with how they are being informed and consulted, resulting in a growing rejection of the benefits of data sharing.

The NDG Review provided an opportunity for Dame Fiona to advance this priority as the Secretary of State asked her to propose a new consent/opt-out model which "*makes it absolutely clear to patients and users of care when health and care information about them will be used, and in what circumstances they can opt out.*"¹⁹

¹⁴ <https://www.gov.uk/government/speeches/reasonable-expectations>

¹⁵ <https://www.sheffield.ac.uk/faculty/social-sciences/making-a-difference/sheffield-solutions>

¹⁶ <https://www.gov.uk/government/publications/sharing-data-in-line-with-patients-reasonable-expectations>

¹⁷ <https://www.connectedhealthcities.org/>

¹⁸ <https://www.citizensjuries.org/>

¹⁹ From the Terms of Reference for the review, which can be found in Annex A of the report

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

The NDG Review's work on opt-outs built on the principle established in the NHS Constitution, which states: *"You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis."*²⁰

It was also foreshadowed by the IIGOP report in January 2015, which called for "a national policy and guidance on consent and objections to data sharing."²¹

The NDG Review affirmed the principle of patients being able to exercise choice about the use of their personal confidential information and 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."*

The recommendation made on publication in July 2016 was to test out two possible opt-outs, one being a single opt-out relating to data used for both running the health and care system and also for research. The other possible opt-out splits these two uses into two separate choices. The Department of Health has been undertaking further work to examine these two options.

This is to be welcomed. As the NDG has made clear, the principle of offering an opt-out is core to building public trust. People need to see they can exercise control and that data is not being used in a way which will surprise them. It is crucial that the opt-out is supported by clear communication with both health and social care professionals and the public, so that people can understand what their data is used for and by whom, and what choices they can make.

The principle that there should be no surprises for the citizen about how their health and care data is being used ran through the work that Dame Fiona and her panel undertook around the care.data programme. On appointing Dame Fiona as NDG, the Secretary of State gave an assurance that no data would be extracted from GP surgeries under the care.data programme until she had indicated that she was satisfied with the proposals and safeguards proposed by care.data²². He had recognised the need to build public trust and that the creation of the role of NDG was key to this. The NDG and her panel continued to liaise with the care.data programme and in January 2015 published a series of questions and tests that should be satisfied²³.

On publication of the NDG Review in July 2016, NHS England decided to close the care.data programme. In a statement to Parliament on 6 July, 2016, the Health Minister George Freeman MP said: *"In light of Dame Fiona's recommendations, NHS England has taken the decision to close the care.data programme. However the government and the health and care system remain absolutely committed to realising the benefits of sharing information, as an essential part of improving outcomes for patients."*²⁴

²⁰ <https://www.gov.uk/government/publications/the-nhs-constitution-for-england/the-nhs-constitution-for-england#patients-and-the-public-your-rights-and-the-nhs-pledges-to-you>

²¹ Recommendation 2, page 46: <https://www.gov.uk/government/publications/iigop-annual-report-2014>

²² <https://www.gov.uk/government/news/national-data-guardian-appointed-to-safeguard-patients-healthcare-information>

²³ <https://www.gov.uk/government/publications/iigop-report-on-caredata>

²⁴ <https://www.gov.uk/government/speeches/review-of-health-and-care-data-security-and-consent>

Another area where the NDG's principle of 'no surprises' has been tested has been the Memorandum of Understanding (MoU) between NHS Digital, the Department of Health and the Home Office²⁵. This agreement sets out a protocol for the Home Office requesting data from NHS Digital for the purpose of tracing individuals suspected of immigration offences. Information which may be disclosed under the protocol includes the last known name and address recorded for individuals on central NHS records; clinical information is not supplied.

The Partridge Review, published in 2014²⁶, examined the security and transparency with which patient data had been gathered and shared with external organisations by NHS Digital (which was known as the Health and Social Care Information Centre at the time). It drew attention to the organisation's National Back Office (NBO) and the facility it offers the Home Office and other government agencies, to gain demographic information about people suspected of law breaking. As a result of the Partridge Review, a review of the NBO was commissioned by the NHS Digital Board and started in 2015.

After the publication of the MoU in January 2017, the NDG and members of her panel met with representatives of NHS Digital, the Department of Health and the Home Office to discuss the agreement and the NBO Review.

Following that meeting Dame Fiona wrote in April 2017 to NHS Digital in a letter which raised points around transparency, the approach taken to tests of public interest, governance, and the potential impact on health seeking behaviour. She shared this letter with Dr Sarah Wollaston, the Chair of Health Select Committee and it was later published by the committee²⁷ alongside a letter to Dr Wollaston in which Dame Fiona wrote:

"In your letter you also ask if I have any concerns regarding the principle of NHS Digital passing details of individuals to the Home Office in the way set out. My panel and I do have concerns about this, as any perception by the public that confidential data collected by the NHS is shared for a purpose that they had not anticipated or without appropriate controls may well lead to a loss of people's trust.

"You will know that I have highlighted the paramount importance of public trust in my recent report, and have long advocated a policy of 'no surprises' for the public about how data is used.

"I believe that trust would have been better maintained had there been more public debate about where the balance should be struck between the public interest in maintaining an effective immigration service and the public interest in a confidential health service before an agreement was made between NHS Digital, the Home Office and the Department of Health. This would have allowed more scrutiny of the reasoning and factors which led to the policy position which has been taken."

In November 2017, the NBO Review report was published²⁸. The National Data Guardian welcomed the step forward in improving transparency of these releases. She noted its recommendation that Public Health England undertake a review of the impact on public

²⁵ <https://www.gov.uk/government/publications/information-requests-from-the-home-office-to-nhs-digital>

²⁶ <https://www.gov.uk/government/publications/review-of-data-releases-made-by-the-nhs-information-centre>

²⁷ <http://www.parliament.uk/documents/commons-committees/Health/Correspondence/2016-17/Correspondence-Memorandum-Understanding-NHS-Digital-Home-Office-Department-Health-data-sharing.pdf>

²⁸ <https://digital.nhs.uk/NBO-tracing-service-review>

health and on health seeking behaviour arising from the disclosure of personal data in relation to the investigation of criminal offences, including immigration offences; the need for this research had been highlighted as a matter of urgency in her April 2017 letter to NHS Digital²⁹.

‘No surprises’ applies to the way that data is used; it also must apply to the way the NDG operates. Transparency and accountability require that as much information as possible is provided to the public about these activities. This is achieved via our website, by the NDG and her panel taking opportunities to engage with members of the public and others with an interest in this area, for instance at events, by working with bodies with a remit to engage patients and the public, and in this report.

Dialogue with the public

The third principle outlined by Dame Fiona on her appointment as NDG was:

The third principle

Third, there is the over-arching issue of the need to build a dialogue with the public about how we all wish information to be used. Many interests need to have voices in the debate. They include:

- *commercial companies providing drugs and services to the NHS*
- *researchers discovering new connections which will transform treatment*
- *those managing the services on which people rely, so that public money is used to maximum value*

During the NDG Review, a wide range of public and patient views were sought through a series of focus groups and an online survey. Eight focus groups with patients and the general public were held, supplemented by a further four evidence sessions which involved patients, service users and carers. These forms of engagement with members of the public were in addition to work with key interested organisations and individuals including NHS organisations, professional councils, central and local government, care providers, charities and commercial organisations.

A new emerging challenge to public trust has been the increasing cyber threat. As the health and social care sector is digitalised, security vulnerabilities of the past, such as misdirected faxes or filing cabinets left unlocked, are replaced by new threats to the security of data. It is vital that these are addressed so that confidentiality is protected, health and care professionals can reliably access accurate information to provide care, and the public can have trust in the systems’ ability to properly handle data.

It was within this context that the NDG Review was asked to develop data security standards that could be applied to the whole health and social care system and, with the Care Quality Commission (CQC), to devise a method of testing compliance with the new standards.

In the interim between completion of the work of these reviews and its publication Dame Fiona and Sir David Behan, the CQC’s chief executive, sent a letter to NHS trusts to emphasise the need to prepare their people, processes and technology to strengthen

²⁹ <http://www.parliament.uk/documents/commons-committees/Health/Correspondence/2016-17/Correspondence-Memorandum-Understanding-NHS-Digital-Home-Office-Department-Health-data-sharing.pdf>

defences against cyber-attack.³⁰ It outlined responsibilities for protecting patient data, emphasised the need for strong leadership and cautioned against the continued use of unsupported systems.

The NDG Review report set 10 new data security standards, with recommendations for embedding them in every organisation handling health and care information and for introducing tougher sanctions for malicious or intentional data security breaches.

When the NDG Review was published, steps were taken to begin to implement the recommendations ahead of the formal Government response, including the introduction of a requirement within the NHS Standard Contract from April 2017, to implement the NDG Review recommendations on data security and work to redevelop the Information Governance Toolkit.

The increased attention on cyber security and the role that the NDG has played in this has been recognised as vital in managing the WannaCry cyber attack of May 2017, which affected a significant number of NHS organisations. The Department of Health wrote to the NDG a week later, recognising the contribution of her leadership in ensuring most organisations remained unaffected by the attack and were able to keep services running.

To build on the engagement started while the review was underway, the NDG recommended that the Department of Health should conduct a full and comprehensive public consultation on the NDG Review proposals. This took place immediately after the review was published and the NDG was pleased to observe that the number of responses numbered more than 670. Dame Fiona and panel members also took part in three further public engagement sessions held as part of the consultation process.

The NDG Review also recommended that professional bodies and patient representative groups should be involved in further testing of the opt-out with the public and professionals. These recommendations were accepted and the subsequent formal government response issued in July 2017 committed that the opt-out would be robustly tested and developed collaboratively with the public and professionals.

The NDG and her panel members have been very pleased to see the development of Understanding Patient Data³¹ an initiative which aims to support conversations about the use of health and care data and which was started as a result of the NDG Review. It has been examining how best to inform people about the use of patient data and what is most useful to them when taking decisions. The vocabulary and case studies it has produced have already proven useful to the NDG and other bodies. The research and resources produced by the project will be very valuable in enabling the building of a common and accessible language to help patients understand how data is used, the benefits of data use and the choices that they can make.

During the work conducted by Understanding Patient Data, it has found strong support for the use of patient data. This echoes the evidence found by the NDG Review and other studies of public support for the use of health and care data. The NDG and her panel have heard similar messages from Healthwatch England, which has shared insight from research they have conducted about how people think and feel about the way their health and care data is used.

³⁰<http://www.cqc.org.uk/sites/default/files/20160519%20An%20update%20from%20the%20Care%20Quality%20Commission%20and%20National%20Data%20Guardian.pdf>

³¹ <https://understandingpatientdata.org.uk/>

However, engagement with the public consistently shows that alongside that support, there is also concern about which organisations can use patient data for what purpose. 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.

The NDG Review recognised these concerns when it recommended that patients should be given robust assurances that their data will never used for marketing or insurance purposes without their consent. It also called for criminal penalties for deliberate and negligent re-identification of individuals; the Data Protection Bill introduced after the 2017 general election incorporates provisions to do this. The Care Act 2014 also went some way to addressing these concerns by outlawing the provision of patient data for solely commercial purposes such as insurance. However, the provision only applies to data disseminated by NHS Digital. More recently, the NDG has welcomed the proposal in Sir John Bell's recent report to the Government *Industrial Strategy: Life Sciences*³² for a regulatory and commercial framework capable of ensuring that the value of innovations, built for example on algorithms generated using health data, is properly recognised by the NHS.

Acting from the viewpoint of the citizen, the NDG and her panel need to keep closely in touch with public opinion and views. Finding innovative ways of doing this remain a priority, whether it is commissioning a citizens' jury, conducting a survey working with patient representative groups or participating in engagement sessions led by other organisations³³. The public conversation the NDG continues to advocate is one that many organisations need to conduct on an ongoing basis. As the NDG Review states, the case for data sharing still needs to be made to the public, and all health, social care, research and public organisations should share responsibility for making that case.

Working with others

Dame Fiona Caldicott has repeatedly emphasised the importance of dialogue with the public. She also places immense importance on working with other organisations and groups which take an interest in the use of patient data.

Representatives of many organisations have come to meet the NDG and her panel members to seek advice on projects, update members on work they are doing and to consult on issues of concern and common interest. These organisations have included NHS England, NHS Digital, the British Medical Association, the Royal College of GPs, the National Aids Trust, Genomics England, Doctors of the World, Liberty, the Information Governance Alliance, Cancer Research UK, Macmillan Cancer Support and Healthwatch England.

As outlined above, the NDG has worked with the University of Sheffield's Sheffield Solutions on two seminars to examine how data might legitimately be shared so that care can be provided. Exploring further the public attitude to sharing health data, a citizens' jury will be carried out in partnership with Connected Health Cities³⁴ and Citizens Juries CIC³⁵ to examine more closely the reasonable expectations of the public.

³² <https://www.gov.uk/government/publications/life-sciences-industrial-strategy>

³³ For example, <http://www.involve.org.uk/2017/07/17/theres-benefits-talking-data-sharing/>

³⁴ <https://www.connectedhealthcities.org/>

³⁵ <https://www.citizensjuries.org/>

As described above, the NDG and her panel have been supportive of the Understanding Patient Data project³⁶ in its work to support better conversations about the uses of health information

The NDG has also provided evidence and opinion to the Health Select Committee, the Science and Technology Select Committee and the Lords Committee on Artificial Intelligence on issues such as big data³⁷, the Digital Economy Act, the release of demographic data by NHS Digital to the Home Office for immigration enforcement and the development of artificial intelligence.

During the past year, the UK Caldicott Guardian Council³⁸ has become a sub-committee of the NDG Panel. The council aims to be a point of contact for all Caldicott Guardians and for health and care organisations seeking advice on the Caldicott principles, to enable Caldicott Guardians to share information and experience, to encourage consistent standards and training for Caldicott Guardians and to help develop guidance and policies relating to the Caldicott principles. This relationship has allowed the NDG to offer support on work such as the production of a new Manual for Caldicott Guardians³⁹ and the NDG to draw on the expertise of a network of Caldicott Guardians working at the frontline in a range of organisations.

There are important alliances that the NDG has with the Information Commissioner's Office (ICO) and the Care Quality Commission (CQC). Both CQC and the ICO are regulators, whereas the NDG role is to advise and challenge. Clearly, the effectiveness of the NDG role relies on close working relationships with these bodies.

As discussed above, the NDG collaborated with CQC over the development of the data security standards recommended in the NDG Review. From September 2017, the CQC began to include these standards into inspections of NHS trusts, with other NHS organisation to follow in a staged way.

One of the issues where the NDG has liaised closely with the ICO has been over the work DeepMind Health has done with the Royal Free London NHS Foundation Trust in developing and testing an app to track acute kidney injury. During the project personally identifiable data relating to 1.6 million patients was used on a legal basis of implied consent for direct care.

The Information Commissioner asked the NDG to give advice on the use of this common law legal basis. Her view was that this legal basis was not appropriate; it would not match with patients' reasonable expectations about how their information might be used⁴⁰. This was a core element of the ICO investigation and decision, delivered in July 2017. It found that the Royal Free had broken Data Protection law and that it should commit to changes⁴¹. The ruling supported the NDG view that patients would not reasonably expect their records to be used in this way. It also raised important issues about the efforts made

³⁶ <https://understandingpatientdata.org.uk/>

³⁷ <https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2015/big-data/publications/>

³⁸ <https://www.gov.uk/government/groups/uk-caldicott-guardian-council>

³⁹ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf

⁴⁰ <https://www.gov.uk/government/publications/request-for-correspondence-between-the-ndg-and-the-royal-free>

⁴¹ <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/>

to inform patients about the project. This is a valuable example of how the NDG role complements and contributes to work of regulators which have enforcement powers.

During and after this case the NDG recognised that more guidance is needed for those developing technology. Brilliant technical innovation will deliver better care to patients and innovation needs encouragement, not stifling. However, the legality of any activity must be maintained if the public are to have confidence in the use of data. The Department of Health has agreed that this guidance is needed and has committed to providing it.

Independence

Just as trust is at the heart of securing public confidence, it is equally required in the relationship between independent advisor and government. Each needs to know they will not spring a surprise or change their plan without informing the other; that disagreements are handled with integrity; that independence requires the government to listen to advice and change. The NDG reserves the right to speak freely and independently if it appears that significant issues and discussions are failing to reach the public. The placing of the NDG on a statutory footing will further underline the importance of there being a person of independent standing who is able to challenge and the health and care system about the use of data on behalf of the public.

Outlining the proposal to place the role on a statutory footing in September 2015, the Secretary of State said:

“The NHS has not yet won the public’s trust in an area that is vital for the future of patient care.

Nothing matters more to us than our health, and people rightly say we must be able to assure the security of confidential medical information.”⁴²

The Government consulted on the roles and functions of the National Data Guardian between September and December 2015⁴³. In July 2016 it published its response to that consultation⁴⁴, which made clear that broad support had been expressed for the role and for making it statutory by a range of stakeholders including health and care professionals, patient groups, privacy campaigners and professional groups. In that response, the Government confirmed its intention to provide a firm legal basis for the role, saying:

“By establishing the National Data Guardian in law, the Government will send a clear message that the concerns and views of the public will be heard and reflected back to health and care organisations. It also provides a means by which the National Data Guardian function will be embedded into the work of the health and care system and sustained in future years. Whilst the National Data Guardian will seek to influence and encourage positive change, it is important to put beyond doubt that the role will not simply be to lobby for change but to hold individuals and organisations to account for how they use and share people’s data.”

⁴² <https://www.gov.uk/government/news/health-secretary-outlines-vision-for-use-of-technology-across-nhs>

⁴³ <https://www.gov.uk/government/consultations/the-role-of-the-national-data-guardian-for-health-and-social-care>

⁴⁴ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535158/NDG_consultation_response_A.pdf

In the absence of relevant health legislation, the Government supported the introduction of Private Members' Bill by Jo Churchill MP, in November 2016⁴⁵. However, the process of this becoming law was not completed before Parliament was dissolved for the general election in June 2017. During that election there was a commitment within the Conservative Party manifesto to place the role on the statutory footing and the commitment was reiterated in the Government response to the NDG Review published in July 2017⁴⁶.

In the new Parliament, a Private Members' Bill to place the role on a statutory footing has been introduced by Peter Bone MP⁴⁷ and at the time of the publication had passed through its second reading on 1 December 2017. The NDG is optimistic that legislation will be passed in this Parliament to provide her with statutory powers, particularly given there is cross-party support for the role being made statutory.

Although the NDG has been able to carry out her duties with unfettered independence, statutory authority would require organisations in the health and care system to take account of her recommendations. The IIGOP report⁴⁸ said in January 2015: *"In summary, the goal should be a state of information governance in which the following proposition prevails: Organisations have no hiding places, the public have no surprises."* Statutory recognition would remove the hiding places and reduce the scope for public surprise.

Looking ahead

Clearly the NDG role has had impact. As innovation proceeds and new pressures develop on health and social care the role is as important as ever. There is a need to provide guidance which creates openness and discussion with the public. The enormous gains that can be made through the use of patient data must not be blocked. Neither should new projects fall down because they have failed to build public confidence and take people with them.

By retaining independence it has been possible for the NDG to make a valuable contribution to building trust. If the NDG became seen as an arm of government, the role would become weakened and lose credibility. The NDG is not a regulator and is not intended to be one; regulators already exist. Rather, the role involves initiating conversations and interventions which ensure the generators of information, the citizens, feel informed and in control of how it is used.

This report has aimed to make accessible the work of the NDG, endeavouring to ensure accountability for the role. By providing the public with a means to assess her impact and influence, it becomes possible for people to measure activity since 2014 against the three principles of sharing, 'no surprises' and dialogue.

The NDG has laid out the following priorities for the next year in advance of the role being placed on a statutory footing:

- 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.**

⁴⁵ <https://services.parliament.uk/bills/2016-17/healthandsocialcarenationaldataguardian.html>

⁴⁶ <https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care>

⁴⁷ <https://services.parliament.uk/bills/2017-19/healthandsocialcarenationaldataguardian.html>

⁴⁸ Page 47: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/391533/iigop-annual-report.pdf

A first key element of this is the successful implementation of the National Data Guardian's Data Security standards. Demonstrating that information systems are secure, well-protected against cyber crime and accessible to those who are providing care directly to individuals, is a necessary step in building trust. Building this into all health and care provision needs local leadership as well as national direction. There has to be both encouragement and sanctions and the introduction of the new Data Security and Protection Toolkit will be important in the coming year.

Secondly the opt-out must offer a genuine choice to be a powerful tool in creating and sustaining public confidence. It can demonstrate to citizens that their wishes are being valued and their concerns are being acknowledged

- 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.**

Promoting the public and patient point of view will remain vital if trust and confidence is to build. With a foundation of strong public support, innovation will develop and accelerate, producing exciting progress in the quality of care and medical research.

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

This will include the continuation of conversations with relevant stakeholders about the NDG's concerns over the way that demographic data is released by NHS Digital for immigration enforcement as laid out in the Memorandum of Understanding with the Department of Health and the Home Office. It will also include feeding into the work planned to revise the Department of Health's Confidentiality: Code of Practice 2003.

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

This should include consideration of the proposal in Sir John Bell recent report to the Government *Industrial Strategy: Life Sciences*⁴⁹ for a regulatory and commercial framework capable of ensuring that the value of innovations, built for example on algorithms generated using health data, is properly recognised by the NHS. As Dame Fiona discussed with the Lords Select Committee on Artificial Intelligence⁵⁰, such an approach may help to address some of the public concern expressed about commercial organisations using health and care data and underlined the need for more discussion with the public about this.

- 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.**

⁴⁹ <https://www.gov.uk/government/publications/life-sciences-industrial-strategy>

⁵⁰ <http://www.parliament.uk/ai-committee>

To include work to consider the consistency of requirements under common law and data protection law.

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

Relationships with the CQC and ICO remain vital. As the Data Protection Bill progresses, it will be important also to liaise with the Department for Digital, Culture, Media and Sport. The Bill will bring in the European Union's General Data Protection Regulation (GDPR) and endeavour to build and maintain protection of citizens' data.

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.