NDG National Data Guardian
for health and social care

Consultation background document

Caldicott Principles: a consultation about revising, expanding and upholding the principles

Consultation runs June 25 to September 3

Overview

Background to the Caldicott Principles and Caldicott Guardians

The Caldicott Committee's Report on the Review of Patient-Identifiable Information published in 1997[1] recommended six good practice principles to be applied to the use of confidential information within the NHS. It also recommended that a senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information.

The principles became known as the Caldicott Principles. And the senior individuals responsible for ensuring that the principles were upheld within their own organisations became known as Caldicott Guardians.

Every NHS organisation has had to have a Caldicott Guardian since 1998, and each local authority with adult social care responsibilities has been required to do so since 2002. The principles and the Caldicott Guardian role are also used by other organisations within the health and social care sector, such as care homes and hospices, and by some organisations in other sectors such as prisons, police and armed forces.

The *Information Governance Review*[2], published in 2013, reviewed the principles and found that they had become well-established and were considered a clear and simple guide to how confidential information should be handled. It also found that Caldicott Guardians still played an important role in helping their organisations to act ethically and legally. and comply with the law.

The 2013 review also introduced a new Caldicott Principle to encourage information sharing in the best interests of patients and service users and users of social care services:

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

[1] https://webarchive.nationalarchives.gov.uk/20130124064947/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf
[2] https://www.gov.uk/government/publications/the-information-governance-review

The importance of applying this new principle to data sharing for individual care was later reflected in law in the Health and Social Care (Safety and Quality) Act 2015[3].

Why we are consulting

The National Data Guardian for Health and Social Care (NDG) is now seeking views on:

- Proposed revisions to the seven existing Caldicott Principles;
- Proposed extension of the Caldicott Principles through the introduction of an additional principle which makes clear that patients' and service users' expectations must be considered and informed when confidential information is used;
- The proposal that the NDG uses her statutory power to issue guidance about organisations appointing Caldicott Guardians to uphold the Caldicott Principles.

The work leading up to this consultation has been taking place for over two years. These proposals are not a response to the COVID-19 coronavirus pandemic or the data sharing arrangements that it has prompted. However, we are clear that there will need to be careful consideration after the pandemic's emergency response is over of which temporary data sharing arrangements should end; what is appropriate during a public health crisis to meet the overriding need to protect the public may not be appropriate when the danger recedes. Equally, some of the changes that have been introduced at speed to improve data sharing may be very beneficial and should be maintained.

We hope that by conducting our consultation now we can develop a new set of Caldicott Principles and guidance in time to inform decisions and discussions about data sharing after the pandemic is resolved.

If you would like to discuss the consultation, please contact the Office of the National Data Guardian: ndgoffice@nhs.net

Revising and expanding the Caldicott Principles

Proposed revisions to the existing Caldicott Principles

During the preparatory engagement that she carried out before issuing this written consultation, the NDG heard that the existing Caldicott Principles remain useful and relevant. We have been told by stakeholders that the principles still have useful functions in helping both staff and organisations understand their responsibilities in relation to information sharing, in guiding decision making, and in providing a simple summary for staff, patients and service users about how information may be used. We also heard that Caldicott Guardians have an important role to play: for example, in emphasising the continued importance of the common law duty of confidentiality alongside other requirements, such as data protection law.

During work to consider the addition of a new principle, the NDG has taken the opportunity to review the wording of the existing principles. As a result, the NDG is

[3] http://www.legislation.gov.uk/ukpga/2015/28/section/3/enacted

proposing some amendments to the existing principles in order to ensure that: they are as clear as possible consistent with other data sharing requirements and guidance; and that the language is up-to-date.

You can see the proposed new set of eight Caldicott Principles in Annex A of this document. In Annex B we have provided the previous seven Caldicott Principles marked up to help you see what amendments we are proposing.

Proposed expansion of the Caldicott Principles

The NDG is proposing to introduce a new principle, which emphasises the importance of there being no surprises for patients and service users with regard to the use of their confidential health and care data.

This proposal is the next step in work that the NDG and her advisory panel have been progressing for several years. Their work has involved a close and careful consideration of the role that the legal concept of 'reasonable expectations' should play in shaping the circumstances under which health and care data may be legitimately shared.

This has encompassed articles[4]; seminars[5] with health and care professionals, legal experts, ethicists, academics, and patient representatives; a citizens' jury[6]; discussions among the NDG panel and with stakeholders. These discussions have also been informed by academic work led by two NDG panel members, Dr Mark Taylor and Professor James Wilson, which resulted in the publication of *Reasonable Expectations of Privacy and Disclosure of Health Data*[7]*.* This article demonstrates that since the Human Rights Act 1998 came into force, courts have developed the significance of the concept of a 'reasonable expectation of privacy' within the law of confidence. It argues that one result of this is to provide an alternative route for the lawful disclosure of confidential patient information, where there is no reasonable expectation of privacy.

In early 2019, the NDG conducted a consultation[8] which asked for views on the work priorities that she should be pursuing once the NDG role moved to a statutory footing[9] later that year. Around 80% of those who responded agreed that *Safeguarding confidentiality* and *Information sharing for individual care* were areas that the NDG should prioritise. The rationale being that these are integral to the NDG's remit to maintain and build public trust, and to enable data sharing within a clear legal and ethical framework.

The consultation responses reflected a demand for clearer guidance, greater simplicity (to support clear and confident decision making around the use and sharing of data, and clarity for the public. There was also support for the NDG's proposals to review the existing Caldicott Principles, so as to give further clarity and to support appropriate information sharing.

---

[4] For example https://www.gov.uk/government/speeches/reasonable-expectations and https://www.gov.uk/government/speeches/exceeding-expectations
[5] https://www.gov.uk/government/publications/sharing-data-in-line-with-patients-reasonable-expectations
[3] https://www.gov.uk/government/speeches/talking-with-citizens-about-expectations-for-data-sharing- and privacy
[7] https://academic.oup.com/medlaw/article/27/3/432/5479980
[8] https://www.gov.uk/government/consultations/national-data-guardian-a-consultation-on-priorities
[9] https://www.gov.uk/government/news/dame-fiona-caldicott-appointed-as-the-first-statutory-national-data-guardian-for-health-and-social-care

The NDG believes that a number of benefits would result from the introduction of a new principle which makes clear that patient and service user expectations must be considered and informed when confidential information is used. Introducing this next principle would:

- Be consistent with the direction that the courts have taken in making an individual's reasonable expectations of privacy the touchstone of the duty of confidentiality
- Add an explicit reference to the NDG's long-standing view that there should be 'no surprises' for the public in regard to how their confidential information is being used
- Align with the General Data Protection Regulation (GDPR) emphasis on transparency and data subject rights
- Align with professional guidance such as the General Medical Council's *Confidentiality: good practice in handling patient information*[10]
- Reflect the welcome move in recent years away from a paternalistic 'doctor knows best' approach to care and towards a partnership approach between health and care professionals and those in their care.

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

Our consultation questions 5 and 6 seek views on the new proposed Caldicott Principles and proposed amendments to the existing principles.

Upholding the Caldicott Principles: the role of the Caldicott Guardian and NDG statutory power to issue guidance

The role of the Caldicott Guardian

NHS organisations have been required to have a Caldicott Guardian since 1998. In 2002 councils with responsibilities for social services were instructed to appoint a Caldicott Guardian by way of Local Authority Circular: LAC(2002)2.

Although organisations in both the NHS and social care sectors were instructed to appoint Caldicott Guardians, it was left to individual organisations to determine how they would operate. We are aware that many other organisations have chosen to appoint Caldicott Guardians or have a Caldicott Guardian function, both within the health sector and more broadly, for example; private healthcare providers, residential care homes, hospices, and organisations delivering domiciliary care.

The UK Caldicott Guardian Council (UKCGC)[11] provides support for Caldicott Guardians and others fulfilling the Caldicott function within their organisation. The UKCGC is not a professional body and does not have responsibility for regulating Caldicott Guardian

[10] https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality
[11] https://www.gov.uk/government/groups/uk-caldicott-guardian-council

activities. Instead it works as a point of contact for the more than 18,000[12] Caldicott Guardians in the UK, enabling the sharing of information, views and experience; encouraging consistent standards and training; and helping to develop guidance and policies relating to the Caldicott Principles.

The UKCGC produced *A Manual for Caldicott Guardians* in 2017[13], which gives an overview of the role of the Caldicott Guardian. It points out the diversity of the organisations in which guardians work, and the great variety of ways in which the role is performed because of this. The manual outlines that:

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

The Caldicott Guardian should play a key role in ensuring that their organisation satisfies the highest practical standards for handling person-identifiable information. Their main concern is information relating to patients, service users and their care, but the need for confidentiality extends to other individuals, including their relatives, staff and others.

...Caldicott Guardians should apply the principles wisely, using common sense and an understanding of the law. They should also be compassionate, recognising that their decisions will affect real people — some of whom they may never meet. The importance of the Caldicott Guardian acting as "the conscience of the organisation" remains central to trusting the impartiality and independence of their advice.

The manual makes clear that it is not possible to provide a single job description for Caldicott Guardians because of the differences in how the role is carried out, as previously mentioned. But it nonetheless provides information on the Caldicott Guardians' responsibilities, including for safeguarding and clinical safety, accountability and key relationships, such as with the Senior Information Risk Officer (SIRO). Since the incorporation of GDPR in UK law in 2018, the Caldicott Guardian's relationship with the Data Protection Officer has also become very important. The manual provides advice about the support that organisations should provide to their Caldicott Guardians, core knowledge needed, and how to learn and develop as a Caldicott Guardian.

NDG statutory power to issue guidance

The National Data Guardian is seeking views on the proposal that she uses her statutory power[14] to issue guidance that all health and adult social care organisations should appoint a Caldicott Guardian.

Organisations in scope:

[12] Based on evidence provided to the Data Security and Protection Toolkit, August 2019 and the Caldicott Guardian Register maintained by NHS Digital: https://digital.nhs.uk/services/organisation-data-service/services-provided-by-the-organisation-data-service#register-and-directory-updates

[13] https://www.ukcgc.uk/manual/contents

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

The NDG's power to issue statutory guidance comes from the Health and Social Care (National Data Guardian) Act 2018[15]. This Act establishes a National Data Guardian for Health and Social Care, to promote the provision of advice and guidance about the processing of health and adult social care data in England. It outlines that the NDG may publish guidance and that organisations in scope must have regard to such guidance.

The range of organisations that choose to place within scope of her guidance are public bodies within the health and adult social care sector (and organisations which contract with such public bodies to deliver health or adult social care services) in England, where relevant to their functions. When issuing guidance, the NDG may specify which organisations are in scope; it will not always be appropriate for all NDG guidance to apply to the full potential range of organisations.

In this specific case, we are proposing that the guidance would apply to the full range of organisations which could be in scope the NDG powers to issue guidance. We have heard that it may not be proportionate for some smaller organisations to appoint a dedicated Caldicott Guardian. We would propose that the NDG guidance makes clear that while all such organisations should have a Caldicott function, in some organisations this may be part of another role or one Caldicott Guardian might serve several organisations (eg a consortium of GPs). Such pragmatic arrangements are already used by some organisations. Likewise, the guidance could specify the types of organisation that should have a dedicated Caldicott Guardian.

The NDG could also take the opportunity to provide other guidance in relation to the Caldicott Guardian role, for instance: about how the role should be carried out, the position of the Caldicott Guardian with regards to the rest of the organisation (e.g. accountability and decision making), and the relationship of the Caldicott Guardian to other key roles such Data Protection Officers and Senior Information Risk Officers (SIROs).

Content of guidance:

When issuing such guidance, the NDG could take this as an opportunity to provide more detailed guidance in relation to the Caldicott Guardian's role, for instance; about how the role should be carried out, the position of the Caldicott Guardian with regards to the rest of the organisation (e.g. accountability and decision making), and the relationship of the Caldicott Guardian to other key roles.

Our consultation questions 7-9 seek views on the continuing importance of the Caldicott Guardian role, the proposal that the NDG uses her statutory powers to issue guidance about organisations appointing Caldicott Guardians, which organisations should be in scope of such guidance, the content of such guidance and what further support might be helpful.

About the National Data Guardian

The National Data Guardian (NDG) role was created in November 2014 to be an independent champion for patients and the public when it comes to matters of their

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

confidential health and care information. The purpose of the role is to make sure that people's information is kept safe and confidential, and that it is shared when appropriate to achieve better outcomes for patients and service users. The NDG does so by offering advice, guidance and encouragement to, as well as scrutiny of, the health and care system in relation to both health and care data, and wherever else it is used.

In December 2018 the Health and Social Care (National Data Guardian) Act 2018 was passed. The law placed the NDG's role on a statutory footing and granted them the power to issue official 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. The NDG may also provide more informal advice about the processing of health and adult social care data in England. Dame Fiona Caldicott, who had held the non-statutory NDG role since 2014, became the first statutory post holder in April 2019.

Annex A: proposed new set of eight Caldicott Principles

These principles apply to the use of and access to confidential information within health and social care organisations, from health and social care organisations to other organisations and between individuals.

Where a novel and/or difficult judgment or decision is required, you should involve your Caldicott Guardian.

Where the term 'confidential information' is used in these principles, this means all information collected for the provision of health and social care services where patients and service users would expect that it will be kept private. In some instances, the principles should also be applied to the processing of staff information. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses.

Principle 1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of confidential information must be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, and decided upon by an appropriate guardian.

Principle 2 - Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) of the use and access to that information The need for patients and service users to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each individual item of information must be considered and justified so that only the minimum amount of confidential information is included as is necessary for a given function to be carried out.

Principle 4 - Access to confidential information should be on a strict need-to-know basis

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

Principle 5 - Everyone with access to confidential information should be aware of their responsibilities

Action should be taken by organisations and individuals to ensure that all those handling confidential information are aware of their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6 - Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that the use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7 -The duty to share information for direct care is 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 patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8 - Inform the expectations of patients and service users about how their confidential information is to be used

A range of steps should be taken to ensure ‘no surprises’ for patients and service users about how their confidential information is to be used - these steps will vary depending on the use. As a minimum, this should include providing relevant and appropriate information - in some cases, greater engagement will be required to promote understanding and acceptance of uses of information. Patients and service users should be given an accessible way to opt out.

Annex B: Previous seven Caldicott Principles, marked up to show proposed changes

New text is shown below in purple and underlined. Deletions are shown in purple and with a line crossing through.

Caldicott Principles

These principles apply to the use of and access to confidential information within health and social care organisations, from health and social care organisations to other organisations and between individuals.

Where a novel and/or difficult judgment or decision is required, you should involve your Caldicott Guardian.

Where the term 'confidential information' is used in these principles, this means all information collected for the provision of health and social care services where patients and service users expect that it will be kept private. In some instances, the principles should also be applied to the processing of staff information. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses.

Principle 1 - Justify the purpose(s) for using confidential information

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

Principle 2 – ~~Don't u~~Use ~~personal~~ confidential ~~data~~ information ~~unless~~ only when it is ~~absolutely~~ necessary

~~Personal c~~Confidential information ~~data items~~ should not be included unless it is ~~essential~~necessary for the specified purpose(s) of the use and access to that information ~~flow.~~ The need for patients and service users to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary ~~personal~~ confidential ~~data~~ information

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

Principle 4 - Access to ~~personal~~ confidential ~~data~~ information should be on a strict need-to-know basis

Only those individuals who need access to ~~personal~~ confidential ~~data~~ information should have access to it, and they should only have access to the ~~data~~ information items that

they need to see. This may mean introducing access controls or splitting ~~data~~ information flows where one ~~data~~ information flow is used for several purposes.

Principle 5 - Everyone with access to ~~personal~~ confidential ~~data~~information should be aware of their responsibilities

Action should be taken by organisations and individuals to ensure that all those handling ~~personal~~ confidential ~~data~~ information ~~– both clinical and non-clinical staff~~ are ~~made fully~~ aware of their responsibilities and obligations to respect ~~patient confidentiality~~ the confidentiality of patient and service users.

Principle 6 - Comply with the law

Every use of ~~personal~~ confidential ~~data~~ information must be lawful. ~~Someone in each organisation~~ All those handling ~~personal~~ confidential ~~data~~ information ~~should be~~ are responsible for ensuring that the ~~organisation~~ use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7 -The duty to share information for direct care ~~can be~~ is 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 and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8 - Inform the expectations of patients and service users about how their confidential information is to be used

A range of steps should be taken to ensure 'no surprises' for patients and service users about how their confidential information is to be used - these steps will vary depending on the use. As a minimum, this should include providing relevant and appropriate information - in some cases, greater engagement will be required to promote understanding and acceptance of uses of information. Patients and service users should be given an accessible way to opt out.