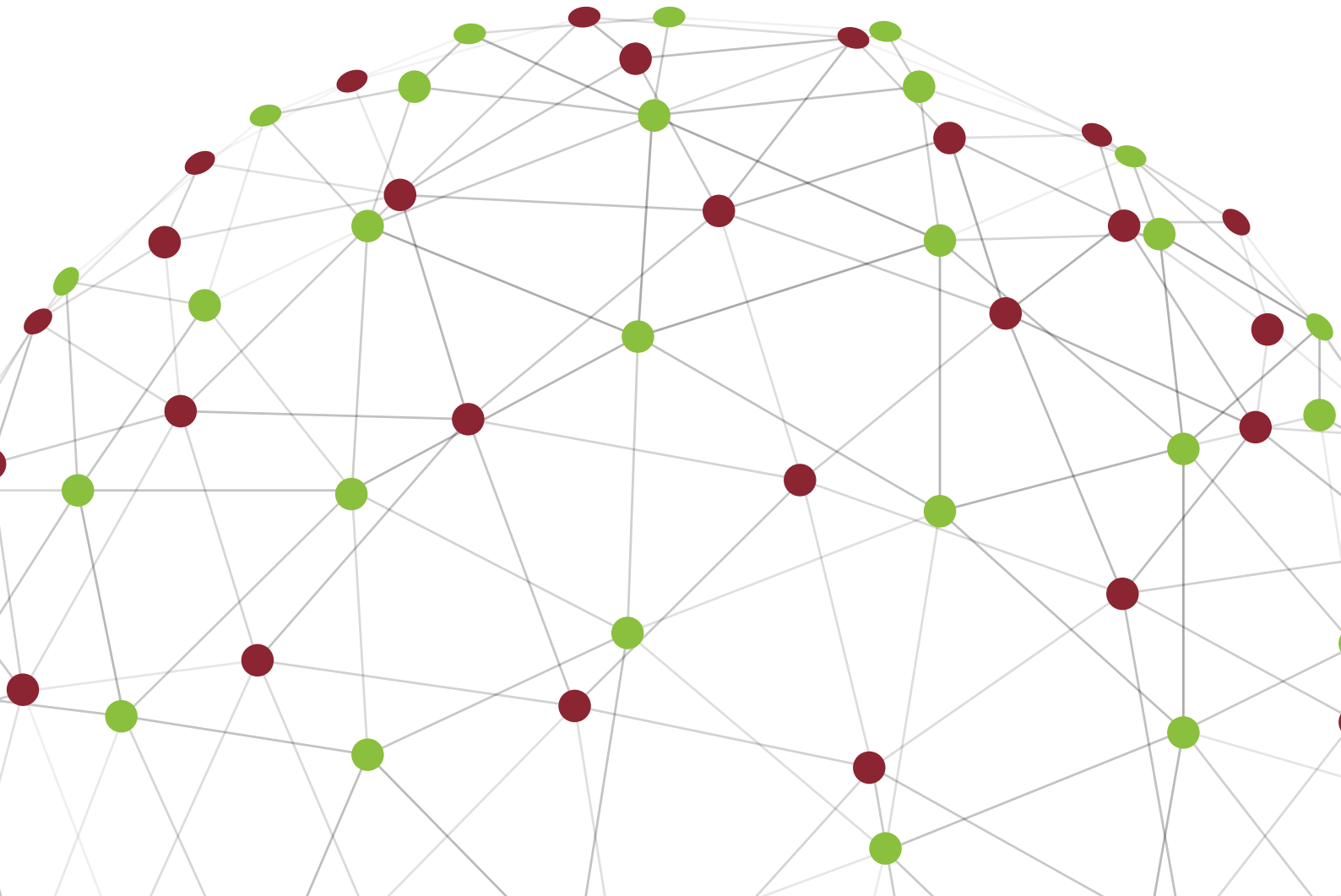
A Manual for Caldicott Guardians

Produced by the UK Caldicott Guardian Council

2017



Contents

Foreword by Dame Fiona Caldicott

When I delivered my report on patient-identifiable information in 1997, I had no idea that it would lead to the appointment of thousands of people to positions bearing my name. That report 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." This recommendation was accepted and since 1998 every NHS organisation has been required to have such an individual in post. It was never my intention that they should be called "Caldicott Guardians", but that became the norm. Frankly I never knew whether to be flattered or embarrassed that so many able people were making wise decisions in my name.

It is too late to change that now. From 2002 local authorities were required to appoint a Caldicott Guardian to ensure that confidential information was protected well and shared wisely in social care. The role has since spread to other organisations in health and social care, and in associated sectors including prisons and the Ministry of Defence. I am told that it has also spread geographically and that Caldicott principles are being followed in other continents.

In recent years the need for guardians has become ever more important. Data about people's experiences of health and social care has huge potential for improving services and discovering more effective treatments and ways to provide care. Those benefits will not be realised without public trust. The Caldicott Guardians are a powerful force for good by making sure that organisations behave in a way that is trustworthy.

I commend this manual, which has been produced by the UK Caldicott Guardian Council to help the guardians address their duties. I have had the pleasure over the years of meeting many guardians and I know that the role is sometimes difficult, but always interesting and rewarding. I would like to take this opportunity to thank all Caldicott Guardians, past and present, for their excellent work.

Dame Fiona Caldicott
National Data Guardian
January 2017

Acknowledgements

This manual has been brought together from contributions by UK Caldicott Guardian Council members Sandra Lomax, Helen Dyer, Sarah Feal, Ben Heal, Stephen Hinde, Council Chairman Christopher Fincken, and with much support from John Carvel. Our thanks and admiration go to those who have shared their experiences for the profiles, to the many who have provided valuable feedback through the manual's gestation, and to Simon Gray and Lindsey Blake at the Office of the National Data Guardian for their encouragement and support.

Edited by Chris Bunch
for the UK Caldicott Guardian Council
January 2017

Every effort has been made to ensure that hyperlinks are accurate. However, Government and NHS websites are undergoing a refit which may break some links. We will endeavour to keep the online version up to date.[1]

1. https://www.gov.uk/government/groups/uk-caldicott-guardian-council

A Manual for Caldicott Guardians

Introduction

1. There are thousands of Caldicott Guardians[1] in health and social care organisations across the UK. They share a common function, which is to make wise decisions about the use of people's information. They balance the need to protect people's confidentiality with the need to protect their welfare by ensuring that information is safely communicated among the various professional teams caring for an individual, sometimes across organisational boundaries. They bring to bear ethical as well as legal considerations, making judgements about real life human situations that could not be done by a machine.
2. However, Caldicott Guardians are not all the same. In a large NHS hospital trust, the Caldicott Guardian may be the medical director, director of nursing or a senior health professional, with wide-ranging professional responsibilities and supported by teams of people expert in information management and governance. In a local authority, the Caldicott Guardian may be a director of similar seniority and with similar support, but with different precepts regarding the consent needed from service users before information about them can be shared. There are Caldicott Guardians in hospices, clinics, care homes and prisons. They are appointed in GP practices, pharmacies and charities. They perform a key role in the largest of the organisations that govern the health and social care sector, but also in the smallest organisations. Some providers and commissioners are required by Government to appoint a Caldicott Guardian; others choose to do so because they want to do their best to look after people's information legally and ethically.
3. Given this diversity, it is not possible to produce a single manual that would provide every Caldicott Guardian with everything they might need to know to perform effectively. The UK Caldicott Guardian Council (UKCGC) offers this relatively short guide in the hope that it will help in various ways: as a starting point for the newly-appointed Caldicott Guardian, as an *aide memoire* for the more experienced, and as a pointer to the possibilities for professional development and support.
4. At the outset, it is worth giving a word of warning. It is difficult to explain how rewarding the work of a Caldicott Guardian can be without giving examples of the activities of individual Caldicott Guardians. We have therefore included a number of profiles of people doing this important work. These are only examples: a case handled by a Caldicott Guardian in one sector may or may not have wider relevance in others. They are not presented as precedents to be followed: the skill of a good Caldicott Guardian is to apply wise judgement to the precise circumstances of each case.
5. An important message to Caldicott Guardians is that they are not alone. Regional and local networks are being established that can provide peer support. It is unrealistic to expect that every small organisation will have wide-ranging expertise in every aspect of information governance. Getting legal advice might put an unreasonable strain on hard-pressed budgets. However, help is often available. For example, the Caldicott Guardian in a GP practice in England may be able to access support from its Clinical Commissioning Group or Commissioning Support Unit. In some cases, there may be a problem without a "right" answer. In such circumstances the Information Governance Alliance (IGA) can be an important source of guidance, and UKCGC stands ready to use its members' experience to offer advice.

1. In Northern Ireland Caldicott Guardians are known as *Personal Data Guardians*.

Adrian Marchbank is Caldicott Guardian for Plymouth Hospitals NHS Trust, a large acute trust whose main hospital has around 1,000 beds and more than 10,000 staff. Since 2000 his main job at the trust has been working as a consultant heart and lung surgeon, handling a busy list of patients and undertaking clinical research. In 2012 the position of Caldicott Guardian fell vacant and Adrian was appointed after competing against other candidates. He says his enthusiasm for the Caldicott work was rooted in a personal experience at the age of 15. After his grandfather died, the local paper printed an article including the name, address and phone number of his grandmother, without seeking her consent. Her obvious distress was Adrian's introduction to issues of privacy and confidentiality. In many NHS trusts, the Caldicott Guardian role is one of the many tasks performed by the medical director or director of nursing. In Plymouth they prefer to appoint a senior clinician who is not on the board. Adrian says that works well for him: he is senior enough to carry clout, but independent enough to act from time to time as "the pebble in the shoe."

He devotes one day a week to the role, setting aside Mondays for routine Caldicott work, including meeting newly appointed doctors, nurses and other staff to induct them into the part they and their teams will play in ensuring a high standard of information governance. He makes himself available at other times, when needed, to deal with cases that are outside the routine and require his personal judgement. The trust has a Senior Information Risk Owner (SIRO) with whom he works very closely, and an information governance team of three, who carry out the day-to-day tasks.

However much of the work to ensure a high standard of information governance is devolved to clinicians and administrators in each of the trust's service delivery units. The trust reports more incidents to the Information Commissioner's Office than most – not because it breaches the data protection rules more often, but because it has a commitment to total transparency and a policy of zero blame. Adrian says: "Mistakes happen. We don't punish individuals, but when things go wrong we look at the processes." One such exercise led to the removal of fax machines from the trust.

Adrian regards the introduction of this devolved and vigilant structure as a significant achievement of the Caldicott Guardian. Individual cases are referred up to him for a judgement call on average about once a week. Serious cases, involving a significant breach of patients' confidentiality, come up perhaps once in six months. The most difficult decisions tend to involve balancing ethical and legal issues. Adrian recalls the complex factors involved in the decision to set up a data base to achieve the optimum outcome for babies requiring care. The system could only work if details about the babies could be provided in a form that might allow them to be identified. And it could only work quickly enough if this was done without waiting for the individual parents' specific consent. After canvassing the views of parents, it was decided that saving lives is more important than protecting confidentiality. The data base went ahead. Adrian is a member of the UK Caldicott Guardian Council and co-chair of the south west regional network of Caldicott Guardians.

Origins

6. Caldicott Guardians derive their name and inspiration from the Government *Review of Patient-Identifiable Information*,[1] chaired by Dame Fiona Caldicott, which reported in December 1997. One of its recommendations was 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 report also set out six principles for determining when confidential information might be used and when it should not. These six Caldicott principles have since helped Caldicott Guardians to make balanced judgements for their organisations.

7. In 2013 Dame Fiona completed an *Information Governance Review*,[2] which has come to be known as the Caldicott 2 report. It confirmed the enduring relevance of the six principles, but added a seventh which says that "the duty to share information can be as important as the duty to protect patient confidentiality." The seven Caldicott principles are shown in the box on page 5. In 2014 Dame Fiona was appointed to be the National Data Guardian for health and social care in England.

8. NHS organisations have been required to have a Caldicott Guardian since 1998 and they were introduced into social care in 2002, mandated in England by Local Authority Circular: LAC(2002)2. The sharing of health information to benefit service users in social care is just as important as it is in the NHS. However, although having a Caldicott Guardian became mandatory in both sectors, it was left to individual organisations to determine how they would operate.

9. Although the NHS is governed separately in England and in the devolved administrations in Wales, Scotland and Northern Ireland, all four nations have chosen to have Caldicott Guardians. There are some differences however: for example, in Scotland Caldicott Guardians are only required in the NHS and there are subtle differences in legislation and common law, although all four are bound by the UK Data Protection Act.

10. This manual has been written by experienced Caldicott Guardians distilling best practice from their experience. The pages that follow include frequent references to what Caldicott Guardians should do and what their powers and procedures should be. In this context "should" represents the considered view of the UK Caldicott Guardian Council. It is a manual of good practice.

The Caldicott Guardian's role

11. 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.

12. 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. Organisations typically store, manage and share personal information relating to staff, and the same standards should be applied to this as to the confidentiality of patient information.

13. Caldicott Guardians should apply the seven 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.

1. http://ukcgc.uk/docs/caldicott1.pdf
2. http://ukcgc.uk/docs/caldicott2.pdf

Alison McCallum is Caldicott Guardian for NHS Lothian, the unified health board that provides services for around 867,800 people in Edinburgh and the Lothians.

The Caldicott role is one of many that she has performed there since 2005 as the Director of Public Health and Public Policy. It is a small but important part of her workload, taking on average 30 hours a month to discharge, excluding committee meetings.

Alison is committed to research as integral to high quality prevention, treatment and care. She can cite evidence of the good that can be achieved by means of safe, ethical analysis of large linked data sets. She acknowledges that sometimes researchers and clinical staff see the application of Caldicott principles as just another process delaying their study. However, in her view, the role of Caldicott Guardian is to be an enabler. This includes allowing research to take place by making sure it is done in the right way.

An example of how patients benefited from this approach came from audit and research into the treatment of subarachnoid haemorrhage.[1] It was important to study the records of all affected patients so that recommendations were not biased by inadvertently excluding those who were more seriously ill. The audit used information from GPs and hospital clinical records, brain scans, nationally collected healthcare data, cause of death certificates and residential data about whether or not people had moved away. She says: “It was an object lesson in learning from the experience of patients in the past to benefit the care of those in the future.”

Alison is particularly well placed to understand the differences in how the system works in Scotland and England. She was Caldicott Guardian in East and North Hertfordshire health authority while Director of Public Health there in the late 1990s.

She says: “There are no differences in the Caldicott principles that operate north and south of the border. But they have to be interpreted according to different legal and healthcare systems. In Scotland, patients agree to the secure use of their data when they register with a GP and they are reminded of how the NHS uses data to improve care when they make use of specialist services. In addition to the requirement to provide prevention and treatment, the NHS (Scotland) Act 1978 identifies research, education and training as health service functions. However, once data moves “beyond the physical or virtual bedside”, it must be de-identified at as early a stage as is practical without compromising care.

Alison approves around 500 Caldicott applications a year including those affecting NHS Lothian and others received in her role as the Chair of the multiagency data sharing partnership. The volume of applications has increased hugely as people have come to understand the potential of clinical data to improve the quality of patient care. She says her seniority and responsibility for the population as Director of Public Health gives her authority to take a balanced approach to risk by agreeing projects that a less experienced colleague might reject or approve without the appropriate safeguards. However, taking a risk is not a matter of bending the rules. Alison’s decisions are reviewed by a governance committee including a non-executive director, a member of the Area Clinical Forum and the Employee Director.

1. http://www.saivms.scot.nhs.uk

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.

14. In all but the smallest organisations the Caldicott Guardian should work as part of a broader Information Governance (IG) function, with support staff contributing to the work required. A key relationship is with the *Senior Information Risk Officer (SIRO)*, described on page 7.

15. The Caldicott Guardian also has a strategic role that it is less appropriate to delegate. This involves representing and championing information governance requirements and issues at senior management team and board level and, where appropriate, throughout the organisation's overall governance framework, including the governance of Information Management and Technology (IM&T). This aspect of the Caldicott Guardian's role is particularly important in relation to the implementation of the digital and paperless agendas.

16. Material in this section may be useful in defining job descriptions for Caldicott Guardians and others responsible for carrying out the Caldicott function.

Responsibilities

17. Strategy & governance: the Caldicott Guardian should champion confidentiality issues at board/senior management team level, should sit on their organisation's information governance board or committee, and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.

18. Confidentiality & data protection expertise: the Caldicott Guardian should develop a strong knowledge of confidentiality and data protection matters, drawing upon support staff working within the organisation's Caldicott and

Guy Van Dichele has worked in local government for over 30 years, latterly as an independent consultant specialising in health and social care. He has held the role of Caldicott Guardian in several local authorities across England working with populations of between 250,000 and 500,000. He has also been a member of the governing body of a Clinical Commissioning Group and has experience of working closely with partner organisations including the NHS, police and fire services, and the voluntary sector.

Guy is a social worker by background and remains registered with the Health and Care Professions Council (HCPC). His roles often include management of front-line delivery of direct care and support. He also often holds the responsibility for safeguarding adults. Protecting the personal data of these people is paramount.

Guy says: "Social work requires working in partnership with a range of other agencies and it is imperative that we ensure we have consent to share information in order to provide the best possible support to both the individual and their families. This is different from the position in many health services where they will need to act in the best interests of the person, sometimes without consent, for example in the ambulance service. Social care is rarely in this position and it is imperative we act lawfully."

Working alongside those responsible for systems and information governance within organisations is of critical importance for the Caldicott Guardian. Guy says: "As Caldicott Guardian the first key task is to ensure that you place yourself on the national register and that the organisation is clear what the role is and that people know how to contact you. Creating a positive culture around information sharing and risks and modelling good behaviours is essential. Breaking down the fears people have in reporting errors is a must – you can't put things right and prevent incidents escalating if you don't know about them!"

Guy identifies three key areas in which he has often needed to advise:

Mental health and the deprivation of liberty. Providing mental health services more often than not requires health and social care to work together and to share information. Applying Caldicott principles often prevents untoward incidents and unnecessary distress to individuals and their families, as well as avoiding the risk of further investigation and fines from the Information Commissioner's Office (ICO). Taking away a person's liberty is very serious and should be applied appropriately and with the right professionals.

Safeguarding adults and working with the police. Guy says he still encounters difficulties with the relationship between local authorities and the police in protecting vulnerable adults. There are differences between the disciplines of dealing with criminality and providing protection. The way through this is, whilst respecting each profession's background and training, to work closely together and build professional relationships outside of an incident so that when issues do occur they can be resolved.

Major transformation and the transfer of services from one provider to another. Since 2010 local authorities have embarked on major transformation programmes with a significant reduction in budgets and personnel. The role of Caldicott Guardian over the last few years has seen an increased requirement to ensure these change programmes understand the risks and comply with the law.

Guy says: "It's important not to just react to incidents that arise, but to proactively scan within the organisation to prevent incidents occurring."

information governance functions, but also on external sources of advice and guidance where available.

19. Internal information processing: the Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation's Caldicott function are detailed in the Information Governance Toolkit.

20. Information sharing: the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential personal information may be shared with external bodies and others with responsibilities for social care and safeguarding. This includes flows of information to and from partner agencies, sharing through IT systems, disclosure for research, and disclosure to the police.

21. Many or all of these responsibilities may be shared with the Senior Information Risk Owner (SIRO: see below), with whom the Caldicott Guardian should work closely.

22. Staff should be advised to seek assistance from the Caldicott Guardian where necessary; typical examples of such situations are:

    - requests from the police for access to people's information;
    - requests from people to delete their records;
    - an actual or alleged breach of confidentiality.

Accountability

23. The Caldicott Guardian role has no statutory basis. It was originally conceived as an advisory role, and to an extent it still is, though Guardians are accountable for any advice given. In practice, many information sharing and disclosure scenarios are decided by the Caldicott Guardian and it is important that these are documented.

24. Where the Caldicott Guardian is an executive director within the organisation, she or he will most likely already be accountable directly to the Chief Executive. Where this is not the case or the individual is not a member of the Board or senior management team, direct accountability to the Chief Executive may still be the most appropriate option, although accountability to a senior executive may be appropriate in some organisations. Accountability to the SIRO is *not* recommended, on the grounds that the SIRO might then overrule the Caldicott Guardian. They should have a relationship of mutual respect and ideally they should be of equal seniority. However, it is the good relationship that matters more than the detail of who does what.

Key relationships

Senior Information Risk Owner (SIRO)

25. Information is a valuable resource: its loss can damage services and reputations, and its misuse can damage individuals and organisations. Managing information risks is something organisations need to do, and be seen to do, well. The NHS information governance framework mandates the appointment of two senior roles, typically at Board or Governing Body level within each organisation. These are the *Caldicott Guardian* and the *Senior Information Risk Owner.*

26. These are distinct but complementary roles. Whilst Caldicott Guardians were introduced to the NHS in 1998 and to social services in 2002, the SIRO role was not mandated for the NHS until June 2008 and local authorities were required to appoint a SIRO later that year. Caldicott Guardians are primarily responsible for maintaining the confidentiality of personal information; SIROs have responsibility for understanding how the strategic business goals of the organisation may be impacted by any information risks, and for taking steps to mitigate them.

27. Caldicott Guardians' activities are particularly concerned with the seven Caldicott principles and the common law duty of confidentiality, whilst the SIRO is mainly involved in ensuring compliance with the Data Protection Act and other relevant legislation. It is important to stress however that these are not absolute distinctions: there is much overlap and close working and partnership between the two is essential.

Tracy Livingstone is Caldicott Guardian at Nightingale House Hospice in Wrexham, north Wales. The role is one of her many duties as Director of Nursing and Patient Services.

The hospice is an independent charity providing specialist palliative care. It has 16 beds for inpatients and runs day care services and out-patient rehabilitation. In addition to 105 members of staff, it has 550 volunteers who look after charity shops and provide other support.

Until last year the role of Caldicott Guardian was performed by the hospice medical director, a consultant in palliative medicine at the nearby Wrexham Maelor Hospital. He acted as Caldicott Guardian to both the hospital and the hospice. When he moved to another hospital, Tracy became Caldicott Guardian for the hospice.

"It has been a steep learning curve," she says. Tracy qualified as a nurse in 1987 and became a director at Nightingale House in 2004, but she had no specialist knowledge of information governance. So the first task was to find out what the job involves.

Using internet searches and advice from the information governance team at the local hospital, she learned the basics. A training course run in London by Hospice UK provided useful learning and the opportunity to build a network of contacts in other hospices.

This has helped Tracy to develop policies and procedures to provide better protection for patients' confidential data. For example, she noted a potential risk in the lists of names and addresses that were provided to the volunteer drivers bringing patients in for day care. Although they did not include detailed clinical information, the identity of people coming in to a palliative care unit was sensitive in itself.

The drivers are now equipped with shredder scissors so they can safely destroy the lists to avoid this information falling into the wrong hands. It was a technique that Tracy learned during the Hospice UK training.

The hospice has developed its own scenario-based training. For example, staff are asked how they would respond if A&E at the local hospital called at 4am on a Sunday wanting the home address where a patient should be returned. Staff discuss the issue and learn that it would be inappropriate to release personal information to help the hospital deal with a transport issue, but it might be ethically and legally correct to share allergy information about an unconscious patient to save a life.

Tracy says: "At present I spend 4-6 days a month specifically on information governance and Caldicott work, but that will probably reduce once we have all the processes that we need."

She thinks the hospice benefits from having its own Caldicott Guardian. "We are a small unit and don't have the pool of expertise that exists in the hospital. But we do have more intimate knowledge of the services we run and we can apply the Caldicott principles to the full. In a small organisation you can flounder so it's really important to make sure that you have a network of expertise and resources to give you support. Don't be afraid to ask for help."

For the most part the legal guidelines and ethical principles that influence the decisions of Caldicott Guardians apply throughout the UK. In Wales they should also have regard to the *Wales Accord on the Sharing of Personal Information*.[1]

1. http://www.waspi.org/

Information governance (IG)

28. Information governance is a broad framework for ensuring and assuring that information is managed legally and safely. It may encompass information risk management, knowledge management, records management, freedom of information and access to information legislation.

29. Caldicott Guardians are an integral part of organisations' arrangements for information governance: their primary concern is *who* should be able to access personal information.

30. In addition to the SIRO, information governance within an organisation may fall to several individuals or roles, for example information governance manager, data protection officer, freedom of information (FOI) officer. Caldicott Guardians need to work closely with their IG team and vice versa.

31. Many organisations will also have information asset owners (IAOs) — usually senior individuals responsible for 'information assets', which may include information systems, databases etc. Caldicott Guardians should be aware of any information assets that store or use person-identifiable information and their owners and, with the SIRO, ensure that the arrangements for their secure use are satisfactory.

Clinical governance

32. Dame Fiona Caldicott has often remarked that information governance and clinical governance are or should be closely-related functions, but historically more often or not they are managed separately with IG being closer to corporate governance. An important role for the Caldicott Guardian is to bridge any gaps between information and clinical governance.

Information management and technology (IM&T)

33. Information technology is a universal aspect of our lives and central to the smooth running of any modern organisation. In many hospital Trusts IM&T is provided in house (though some aspects may be outsourced) but in others — for example local authorities, Clinical Commissioning Groups (CCGs) and GP practices— it is typically managed by a third party. Either way, the governance arrangements for IM&T are critical and should be integrated into the organisation's IG arrangements.

34. Information protection is a core function for both IG and Caldicott Guardians, and close working relationships with IM&T providers are essential. For example, Information Governance, with input from the Caldicott Guardian for aspects that affect the use of personal information, will need to ensure that information protection and security policies are fit for purpose, and that system procurement and data processing contracts are robust and include privacy impact assessments.

External agencies

35. Caldicott Guardians are increasingly involved in their organisations' partnership with external agencies and ideally will have good lines of communication with relevant contacts. The Government has encouraged joined up solutions to many problems, including better support for vulnerable children and adults. It is important for Caldicott Guardians to facilitate this and to ensure that information is shared appropriately, and is proportionate and handled securely. This may require privacy impact assessments, information sharing agreements & protocols, systems for consent and the like but, important though these are, they must not impede the underlying aim to promote positive outcomes for vulnerable individuals.

36. Ill-informed decisions in child protection domestic violence assessments have historically led to neglect, injury and even death. The Caldicott Guardian's ethical view on the primacy of human life and welfare can ensure the correct balance between guarding and sharing such sensitive data.

Neill Jones is the Caldicott Guardian for the William Brown medical centre, a GP practice in Peterlee, county Durham. It is one of 30 practices managed by IntraHealth, a not-for-profit company that operates in various parts of England and Scotland. Neill provides Caldicott support for all of them and acts as Caldicott Guardian for those that do not have one of their own.

This is one of many solutions to a problem that is commonplace in general practice. The GPs are data controllers, who are responsible for the security and confidentiality of their patients' data, but many find it difficult to remain up to speed on information issues as well as on all the latest clinical developments.

Neill has been a GP since 1986. He worked initially as a full-time family doctor, but branched out in 1998 to take on other roles.

His current work pattern includes four clinical sessions a week, when he looks after patients in Peterlee or acts as a locum in other health centres in the InterHealth group, as well as being the group's IT lead and Caldicott Guardian.

Neill's work as a Caldicott Guardian often involves making a judgement call. In a recent case he was contacted by a north-east practice asking how it should respond to a solicitor who wanted a patient's entire medical record to help that patient to make a complaint. All the practice's permanent doctors were on leave and the solicitor insisted on an urgent response.

Decisions in such cases often depend on interpreting the third Caldicott principle – that the minimum amount of personal confidential data should be made available for a particular justifiable purpose. Questions included establishing which part of the record was needed, over how long a period.

In another recent case a practice had mistakenly included in medical notes sent to a hospital the fact that a patient had once been on the sex offender's register. The practice apologised and the hospital agreed to remove this reference from the notes that it held. The patient wanted the reference to be removed from the medical notes held by the GP, but that could not be accepted because the information was accurate and in certain circumstances might become relevant. The patient asked the Information Commissioner's Office to intervene and Neill became involved after the ICO asked the practice to explain itself.

Neill's advice was that the entry should become a private note on the file, not visible to anyone but the individual's GP and accessible only during a consultation with the patient, if appropriate. The ICO and the patient were content with that and so the matter was resolved.

Caldicott work does not take up much of Neill's time. Typically he may give Caldicott-type advice once or twice a week. He also ensures that new starters get appropriate training in these issues. As he puts it: "It's important to try to prevent problems rather than scrabble around when issues arise." So, for example, practice staff are taught not to send a fax without first verifying the fax number by sending through a test message and checking that it has safely arrived.

One of Neill's fellow managers acts as his deputy. He copies her in to all the emails he sends answering Caldicott questions and she has access to his paperwork and relevant documents.

37. Effective collaboration may be impeded by:
    - misunderstandings about what specific data can be shared;
    - uncertainty about mental capacity and consent to share;
    - fear of the consequences of sharing overshadowing the need to share;
    - cultural differences leading to professional mistrust of other agencies' staff.
38. The ideal is a balance between sharing where there is good cause to do so, and withholding when there is not. This would enable an effective, joined-up outcome with a low risk of data breach. Further considerations for safe and effective sharing are given on page 21.

Safeguarding

39. The protection of children and adults from abuse and harm is a major social priority. Effective safeguarding requires the judicious sharing of information about those at risk between the agencies involved, and is a good example of multi-agency collaboration. In some but not all situations sharing information for safeguarding is now mandated by law, and in all instances, appropriate sharing agreements and policies need to be in place. Caldicott Guardians should ensure that these afford appropriate protection for the shared information, and that sharing is proportionate. They may also be asked and should be prepared to advise or adjudicate in specific cases.
40. Most health and social care organisations will have persons responsible for safeguarding. Caldicott Guardians should be aware who they are and work closely with and support them.

Learning and development

41. The importance of specialist training for senior information leadership roles, including Caldicott Guardians and SIROs, has recently been highlighted by the National Data Guardian and the Care Quality Commission (CQC). In addition, the Information Governance Toolkit requires appropriate training and support for Caldicott Guardians.

What does a Caldicott Guardian need to know?

42. Your learning needs as a Caldicott Guardian are individual and depend on many factors such as the type of organisation your Caldicott role supports and the particular challenges that your Caldicott function faces.
43. Undertaking a Caldicott role-focussed SWOT[1] analysis on appointment and annually may help you identify a clear vision of your current strengths, potential developments and areas for improvement, and help inform your own individual learning needs analysis.
44. Things to consider include:

Strengths and weaknesses

- your past experience and existing skills and knowledge;
- your own culture and values and how they influence your thought processes in your Caldicott role;
- your available resources: time, money, commitment;
- your own style of learning, of leadership, of management and how it influences the Caldicott role.

Opportunities and threats

- your stakeholders' engagement and expectations e.g. patients, citizens, staff, colleagues, other organisations;
- organisational values, mission and strategy;
- the skills and knowledge that may already be readily available;
- the knowledge or skills gaps which may adversely affect the Caldicott function;
- the Caldicott interventions you have been responsible for recently;
- organisational resources or engagement: time, money, commitment.

1. Strengths, weaknesses, opportunities and threats

Helen Dyer is Caldicott Guardian for ExamWorks UK, the British subsidiary of a US corporation. She is the company's Director of Nursing and the biggest component of her work is concerned with assessing patients for continuing health care, under contract from the NHS.

Across England, some patients qualify after leaving hospital for continuing health care to be paid for by the NHS, while others receive means-tested support from the local authority, pay for themselves, or do without. The decision about who qualifies depends on a clinical assessment of care needs requiring access to confidential data.

In most parts of England those assessments are carried out by staff from the NHS or local authority, but in some areas the work is contracted out to private sector companies such as ExamWorks UK. Full and accurate assessments depend on having access to the reports and records of every member of the multi-disciplinary team who has had contact with the patient, as well as to documents held by the Clinical Commissioning Group and local authority. The process depends on having good information sharing agreements. Getting them right is one of Helen's concerns as Caldicott Guardian.

She says: "It's really important for me to integrate my Caldicott responsibility throughout my work as Director of Nursing. It's not a bolt-on. I reckon I spend about 10% of my time on Caldicott work, but for the most part I do it in tandem with my other work. I often wear my Caldicott Guardian hat at meetings where I also wear my Director of Nursing hat."

A recent example of a Caldicott intervention came when she was asked to sign off a contract with a Clinical Commissioning Group to give assurance that it complied with Caldicott principles. She said it wasn't the job of a Caldicott Guardian to sign off contracts but to advise. Her advice was that the CCG was planning to send a large volume of confidential personal data without an adequate legal gateway. Nowhere was there evidence that people would be asked to give their consent for data to flow to a private company outside the NHS for continuing healthcare assessment. It was thanks to Helen's vigilance as Caldicott Guardian that the CCG put this right.

She says: "When I first became a Caldicott Guardian, there was nothing to help those of us working in the private sector. At the outset Google was my best friend. I was fortunate that I found out how to attend some excellent Caldicott Guardian training. That was pivotal. It opened up access to networking events where I met other Guardians."

Helen keeps a log of the Caldicott advice that she gives. She makes brief monthly reports on her Caldicott activity to the ExamWorks UK board and to its information governance (IG) board. And, as part of the company's compliance with IG Toolkit requirements, she produces an annual Caldicott plan, which is approved by both boards. Other company activities include rehabilitation services and disability assessments.

She says: "I work closely with our SIRO. We have adjacent desks. When I'm on leave she can deal with things, although given the nature of the work there's very little that can't wait until I get back."

Helen is a member of the UK Caldicott Guardian Council and led the work to set up its regional network in north-east England.

Influencing skills

45. Positive leadership and influencing all stakeholders — from board to frontline staff to regulators — will help to embed information awareness and culture into the organisation, for the benefit of patients/service users and staff.

Legal aspects

46. The sixth Caldicott principle *Comply with the law* can be a challenge for Caldicott Guardians. In larger organisations, access to legal, information governance, and records management advice is readily available, but for smaller organisations this can be problematic. Key legislation is included in Annex C, but an awareness of how the legislation is applied should be included as part of the development of the Caldicott role.

Research and development

47. In some organisations, a significant number of Caldicott decisions are based around sharing information for research purposes. If you work in one of these, ensure you have sufficient knowledge and skills to make these decisions or include this as a development need.

48. A SWOT analysis will inform your learning needs analysis which can then be used to populate your personal development plan for continuous professional development, revalidation and appraisal purposes. Your plan, if you have many roles, may be a holistic one which incorporates your Caldicott role learning needs alongside other needs. Alternatively, you may develop a plan that is solely Caldicott-focused.

49. As well as providing evidence of your learning and development for appraisal or revalidation or CPD, you may also consider writing your plan in such a way that its achievement can be used as evidence for your organisation's IG Toolkit assessment.

50. Your plan for your learning and development should be refreshed annually in response to the Caldicott plan for your organisation.

Where and how can a Caldicott Guardian learn?

51. For Caldicott Guardians, every day is a learning day: learning isn't restricted to attending courses and study days. Other opportunities may include:

- review your Caldicott plan evaluation or Caldicott log and undertake reflection about an area of learning within it. This may be facilitated by a coach or through peer support or clinical supervision and you may choose to write your learning in a redacted diary or portfolio as evidence;
- engage with your local Caldicott Guardian network group and raise questions for discussion;
- consider peer review and coaching as opportunities for learning and development;
- undertake the Caldicott-related modules on the IG Toolkit;
- sign up for newsletters, for example the Information Governance Alliance (IGA) newsletter which includes news and information for Caldicott Guardians;
- undertake audit or research and add to the body of knowledge relating to the Caldicott Guardian role;
- review how the application of the Caldicott principles applies to other learning. For example, if you have recently been involved with a safeguarding issue, what learning is there from a Caldicott perspective?

52. If you do decide a course or a study day will work for you, there are many to choose from. A list of training providers offering face to face *Caldicott Guardian training* is available.[1] Be selective when choosing and consider:

- Does this course provide a Caldicott focus or an Information Governance perspective?
- Is it the most resource effective way to meet my learning needs?
- Is the provider accredited? Respected?

1. https://www.igt.hscic.gov.uk/Caldicott2Training.aspx

In the professional world of **Arun Dhandayudham**, the judicious sharing of service users' sensitive personal data is frequent and appropriate. Arun is medical director and interim joint CEO of WDP (previously known as the Westminster Drug Partnership), a third sector provider of drug and alcohol treatment and recovery services in London, the south-east and east of England.

The charity has about 20,000 people on its books - some on substance misuse programmes in prison or in the community, others using in-patient detox and rehabilitation facilities. In addition to sharing information with staff caring for an individual in the NHS and social services, WDP must often share appropriate patient identifiable data with the prison service, probation and other parts of the criminal justice system.

As Caldicott Guardian, Arun has an important role in deciding when it is appropriate to share. About half of the charity's service users come via the criminal justice system. On arrival they usually already have an assigned probation officer who is entitled to keep in touch with how treatment is progressing. The charity has its own criminal justice workers, some co-located in probation service offices, with authority to input some information into probation IT systems.

As well as being medical director and interim joint CEO, Arun is also responsible for IT and so all the important decisions about hardware and software also come to him. He regards this combination of responsibilities as one of the great benefits of working in an organisation with a turnover of tens of millions, not hundreds of millions. He says: "It is very different from the NHS where everything operates in silos. Here we can work holistically. For example, I look at the security of patient information from end to end. I am responsible for the location and cyber-security of our servers and hardware as well as for the information governance that regulates the behaviour of our 400 staff and hundreds of volunteers."

Such matters can be planned, but other questions arise urgently. Sometimes there are cases involving the police asking for information about whether a particular service user was using their facilities at a particular time. "We ask the police why they would want to know. The answer determines the flow of information. The more serious the need for information (such as a homicide investigation), the more likely it is that we will provide the requested information.

Substance misuse services are commonly provided on contracts that are retendered after 3-5 years. Issues arise when a new contractor takes over from another. What happens to the service users' records? In some areas they are owned by the commissioner and the new provider has to make arrangements to gain access. In other areas the records are owned by the previous provider and negotiations to gain access may be more complex. A balance has to be struck between protection of confidentiality and maintaining continuity of care without compromising quality and safety. In such circumstances it is the Caldicott Guardian's job to oversee the drawing up of information sharing agreements.

Arun does not have a deputy Caldicott Guardian. When he is on leave, urgent questions can be referred to a senior colleague, who is well versed in data protection and Caldicott principles. Advice can also be sought from the legal team. Arun keeps a log of all Caldicott Guardian decisions.

- Have you heard good feedback from other Caldicott Guardians or your local Caldicott Guardian Council network?
- Can you commission something with colleagues to meet your collective needs?

53. Networking/sharing best practice is the best way to avoid the often-cited loneliness of the role. There are two conferences for Caldicott Guardians annually — usually in spring and autumn — and several regional networks which can support your development in your Caldicott Guardian role.

54. Evaluation of all your learning and development activities will enable your continuous development.

55. Consider how to share your learning as well as your experiences with others as a way of spreading good practice.

56. There is a wealth of information available on line: links to some key documents are given below in Annex B.

Appraisal

57. All staff in health and social care are expected to undertake an annual appraisal and this is likely to be the case in other organisations. For medical and nursing staff this is central to revalidation, and it should cover all aspects of your work. In addition to supporting revalidation, the outputs from the appraisal can be used in evidence for your organisation's IG Toolkit return.

58. Caldicott Guardians should be able to provide evidence to their own organisations, to regulators (for example, the Care Quality Commission and the Information Commissioner's Office) and to the public on how they are fulfilling their role and how effectively their organisation is applying the Caldicott principles. They should also be able to demonstrate how their organisation is responding to their advice.

59. In preparing for your appraisal you may wish to consider the following:

How does your Caldicott role add value to your organisation?

60. Without appropriate time and support the Caldicott Guardian role can be perceived as a 'tick box' exercise to achieve compliance, but where the role is supported and appropriate time provided to carry out the role effectively, there can be significant benefits to organisations including:

61. *Improving service users' experience*: a key aspect of the role is to know when information should be shared, taking into account the condition of the patient or service user, and the effect a disclosure would have on them. Organisations should have a privacy statement informing people how information about them will be used, which the Caldicott Guardian should oversee. In addition, promoting the safe use of anonymised data for research will help future generations and medical research plus targeting of services.

62. *Improved efficiency*: working more collaboratively requires information to be shared safely between organisations. By establishing an environment in which the seventh Caldicott principle is at the forefront of the decision making, the duty to share becomes the starting point and an enabler rather than barrier to information sharing, resulting in improved efficiency and thereby lowering costs.

63. *Improving culture*: by publicising decision logs, staff are aware of what information they can share safely and know that they have the support of the organisation for example sharing with the police (how much do staff share?). Promoting the use of privacy impact assessments and regular updating of privacy notices enables 'privacy by design' to be built into the organisation's culture.

64. *Preventing future problems*: by engaging with the Board and the SIRO, in reviewing 'near misses' in information breaches, and engaging in wider networking with Caldicott Guardians such as regional networks, best practice can be established before its absence is identified by regulators (e.g. ICO, CQC) and potential adverse publicity and monetary penalties avoided.

Jenny Belza is the Caldicott Guardian for one of England's largest Clinical Commissioning Groups. NHS Birmingham CrossCity CCG has an annual budget of £1 billion and commissions services for 710,000 people.

Jenny has been its chief nurse and quality officer since it came into being in April 2013. That makes her responsible for ensuring quality of service among providers including primary care, acute trusts and mental health. She also manages safeguarding of children and adults, equality and diversity, continuing healthcare and transforming care for people with learning disabilities. She is a member of the CCG's governing body.

With all these responsibilities, it is perhaps unsurprising that being Caldicott Guardian is a small part of Jenny's workload. She says: "Some weeks I don't spend any time on my Caldicott Guardian role. Some weeks it will take a couple of hours."

The CCG does not itself provide direct patient care and so does not routinely handle patients' confidential personal information. Issues that require the attention of the Caldicott Guardian often involve resolving problems that stand in the way of organisations sharing information appropriately.

A recent example came when NHS England was implementing its policy of moving people with learning disabilities from special hospitals to more personalised care in the community. Jenny worked with two other CCGs, the local authority and NHSE to put in place services for 70 individuals in the Birmingham area. Each had different individual needs and so the commissioning work required detailed knowledge of their personal circumstances.

To make the transfer of responsibility safe and to provide a quality service, all the organisations involved in their care needed to share this information. As Caldicott Guardian, Jenny led the work of drawing up an information sharing agreement.

The purpose was to assist the direct care of the individuals and there was no breach of Caldicott principles. But in Jenny's experience there is often difficulty in achieving appropriate sharing across institutional boundaries. People struggle to overcome an over-cautious instinct not to share, even when sharing is in the best interests of the individual. Those judgement calls are part of the work of the Caldicott Guardian.

Jenny has been a nurse for 36 years and so has extensive professional knowledge of the importance of patient confidentiality, but before coming to the CCG she had no previous experience of being a Caldicott Guardian. She works closely with Dr Masood Nazir, the CCG's Senior Information Risk Owner (SIRO), who also sits on the governing body.

When the CCG was set up, they organised training for themselves in information governance and spent time reading up Caldicott material. They set up an information governance steering group in the CCG to look at policies on training and staffing.

The CCG employs an information governance manager who refers issues to the Caldicott Guardian or SIRO as appropriate. They all sit near each other in the corporate office.

Jenny logs all her Caldicott Guardian decisions on a database, which includes all the information sharing agreements that involve the CCG. The information governance manager has access to the log.

There are 110 GP practices in the CCG and sometimes they may call Jenny for advice. She attended the UK Council of Caldicott Guardians' annual conference last year, at which Dame Fiona Caldicott spoke about the importance of appropriate data sharing.

What training and development do you need?

65. Although much of a Caldicott Guardian's work involves plain common sense, there are practical and legal aspects that the Caldicott Guardian must know about or at least be aware of, and evidence of this will need to be available for appraisal. The learning and development section above provides guidance on the knowledge required and how to obtain it.

What support do you need?

66. Annex B provides details of help and support available to Caldicott Guardians. In addition, you should consider the following:

- a deputy: a nominated individual to cover when you are absent. This might be the IG lead, but if so they will need training to enable them to understand the specifics of this role;
- information governance/legal support: to ensure you 'comply with the law' and are actively involved in investigation of breaches and near misses to improve the culture and knowledge of the organisation;
- time to do the job properly – this will depend on the size of your organisation and the scope of your role, but may be anything from one day per month to several days a week.

What evidence should you provide?

67. An important aspect of appraisal for professional revalidation is that you are able to provide evidence for the statements you make in the appraisal document. The following are points to consider:

- training and development attended;
- documentation demonstrating Caldicott decisions made. Note that to date the ICO has not fined an organisation for sharing information inappropriately where relevant risks had been considered, mitigated as far as possible, and documented in a privacy impact assessment (PIA) and/or an information sharing agreement;
- IG Toolkit compliance (if required);
- number of information sharing agreements signed, their purpose, and confirmation that they have an legal basis and are in line with the ICO's code of practice (see Annex B);
- attendance at strategic and steering groups where IG and Caldicott issues are discussed;
- progress with the organisation's Caldicott 2 action plan;
- organisational preparedness for the National Data Guardian's *Review of Data Security Consent and Opt Outs*;[1]
- organisational response to the recommendations of the Care Quality Commission's report *Safe data, safe care,* including robust mechanisms for recruitment and training of Caldicott Guardians, and clarity of accountability for all aspects of data security.

Legal and ethical aspects

68. Caldicott Guardians offer an authoritative view on ethical and human rights and wrongs when considering the sharing of personal data. They seek to find a balance between an individual's privacy and best interests, any risk of harm, and the public good. Their endeavour should result in the best possible answer in the circumstances. Caldicott Guardians are not established by a specific act of parliament and so have no directly related legal basis for their functions. There is however a complex framework of legislation, common law, non-statutory codes of practice and protocols which underpin everything they do.

69. In some complex situations, Caldicott Guardians may need to take legal advice, speak to other Caldicott Guardians or to the UK Caldicott Guardian Council or the Information Governance Alliance before reaching their considered decision. Even if legally permitted, it may not follow that it is ethically right to disclose in particular circumstances. On the other hand, there may be occasions where the legal basis for sharing is unclear or disputed yet there is an overwhelming ethical imperative to disclose. It is important to appreciate that confidentiality is not necessarily absolute, and

1. http://ukcgc.uk/docs/caldicott3.pdf

Julian Mark is Caldicott Guardian for the Yorkshire Ambulance Service, where he has been executive medical director since 2013. On issues of information governance, he seesa big difference between the ambulance service and other organisations in health and social care. The nature of the work is such that it is rarely appropriate to seek the patient's explicit consent for their personal data to be collected and passed on to other members of the direct care team. When paramedics respond to a 999 call, they operate on the basis of implied consent. When they attend to a severely injured person, they do so to look after their best interests without the need for formal consent.

In the day-to-day work of the service, staff do not need to consult the Caldicott Guardian before sharing medical information with other healthcare professionals who need it to provide safe care. However, that does not mean that the role of the Caldicott Guardian lacks interesting challenges.

The issues that come up to Julian often involve requests from other organisations for information that may include personal medical data. For example, police officers often walk into an emergency operations centre and ask for call logs or incident data to assist an investigation into a possible crime. However, files containing personal medical material cannot be handed over there and then unless certain thresholds are reached. The police can make a request for such information under section 29 of the Data Protection Act 1998, but the Yorkshire Ambulance Service will not hand over files until they have been redacted to comply with Caldicott principles. Julian wrote the guidance on this subject that the UKCGC has made available to help others through this delicate process.

Julian's previous clinical career was as an anaesthetist with an interest in trauma and critical care. At the Yorkshire Ambulance Service headquarters in Wakefield his role as executive medical director is concerned with clinical governance and development, improving the quality of the service and assuring patient safety. He says that the role of Caldicott Guardian fits in well with this because it is also about "acting as the patients' champion."

The information governance manager has ready access to Julian who can advise from a Caldicott perspective when issues arise. They meet formally once a month to examine all cases that have been logged as breaches of the rules on protection of patient identifiable data, such as when information about an individual is sent to the wrong GP. Other case work is sporadic. He might look at two issues one week and then none for the next two months. The more significant workload is when agreeing information sharing agreements. For example he spent a fortnight working on the agreement to share information with the Rotherham child abuse inquiry.

Julian has a deputy Caldicott Guardian, who is the deputy medical director. As they never take leave at the same time it makes sense for his deputy to cover both roles. If a member of the public wants to get in touch with the Caldicott Guardian they can find out who it is on the Yorkshire ambulance service website and contact Julian through his PA. He says: "I prefer people to approach me directly rather than going through a somewhat protracted process." Cases are logged on the service's incident reports system and are regularly reported to the board.

health care professionals need carefully to balance the importance of confidentiality against avoiding harm—to the confidant and to others who may benefit from disclosure.

70. The legal aspects which Caldicott Guardians particularly need to be familiar with are the Data Protection Act and the common law duty of confidence. Other relevant legislation is described in Annex C.

The Data Protection Act 1998

71. The Data Protection Act (DPA) 1998 applies to information about identifiable, living individuals. It protects individuals' rights and places legal obligations on organisations. It is presently[1] the primary legislation underpinning the Caldicott Guardian's activities. It relates to personal data, that is data that relates to a living individual from which that individual could be identified — either from that data alone, or from that data in conjunction with other information in the possession of the data controller, or information which would be reasonably accessible to anyone else.

72. The DPA provides eight principles that apply to all use and disclosure of personal information. There is a good concordance between these and the Caldicott principles, and Caldicott Guardians should be familiar with and work to both. In addition to satisfying these eight principles, when processing information organisations must also satisfy one condition from a supplementary schedule and, where the information is deemed sensitive under the provisions of the Act, a further condition from a second supplementary schedule. Where personal information is held in confidence (e.g. health records or case file information) common law obligations additionally require the consent of the information subject before it is disclosed to a third party — unless there is another legal justification, including where exceptional circumstances apply, for example the prevention and detection of crime.

73. The EU General Data Protection Regulation will come into force on 25th May 2018 and will supersede the DPA. The principles are similar to but more detailed those in the DPA and introduce an accountability requirement: it will be necessary to demonstrate how one is compliant with the Regulation. Penalties for data breaches will be significantly increased—up to 4% of annual global turnover (not profit) or €20 million – whichever is the greater.

The Data Protection Act principles

1. Personal data must be processed fairly and lawfully;
2. Personal data must be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Personal data must be adequate, relevant and not excessive;
4. Personal data must be accurate and, where necessary, kept up to date;
5. Personal data processed for any purpose or purposes must not be kept for longer than is necessary;
6. Personal data must be processed in accordance with the rights of data subjects;
7. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
8. Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

1. In May 2018 the DPA will be superseded by the EU General Data Protection Regulation. See Annex C.

Martin Crook is Caldicott Guardian at University Hospital Lewisham and Greenwich (UHL), where he is a consultant chemical pathologist and metabolic physician. His multiple clinical responsibilities include holding four clinics a week in lipidology and metabolic medicine, two of which are held at Guy's and St Thomas' hospitals. He is involved in a hospital nutrition team and is head of department at Lewisham biochemistry laboratory. Martin is also a visiting professor in clinical biochemistry at two universities and has about 200 publications and seven medical textbooks to his name. To make it possible for him to discharge Caldicott Guardian responsibilities in addition to these other extensive duties, Martin has found it useful to work with a hospital 'Caldicott team' comprising colleagues expert in information governance, medicolegal matters, computing and administration.

Martin says: "One of my interests is medical ethics. I did an MA in ethics and law at Keele University, which included writing a dissertation discussing the risk of absolute medical confidentiality. Of course patient confidentiality is extremely important, but it needs to be wisely delivered to reduce third party harm or even detriment to the patient. This is particularly important for example when it comes to genetic information and inherited disease."

This issue is of more than academic interest. Increasingly questions about the ownership and use of genetic information are posing practical dilemmas for the Caldicott Guardian. For example, what if a patient with a genetic lipid disorder e.g. familial hypercholesterolaemia doesn't get on with other family members and thus doesn't want to share information with them? If there is no sharing of information with the relations, they will not be made aware of the risk they may have of also having the condition. Careful and open discussion with patients on a case by case basis can sometimes help under such circumstances as well as applying the Caldicott principles

Martin says: "I have an interest in Caldicott issues raised about access to laboratory results. Should patients sometimes be denied access to their own results? When may the results be shared with others, e.g. HIV results? And how do we guarantee the confidentiality of patient results on IT systems?"

The Caldicott Guardian can help to devise robust systems to help staff deliver services in ways that are both efficient and compatible with Caldicott principles. Martin says: "I work in very busy hospitals serving an inner city deprived multicultural population. Doctors have lists of patients in their care, which can get lost if they are in paper format. I have been looking at the use of electronic means to try and avoid this problem. I have also worked on how we dispose of patient identifiable information, e.g. waste bins, shredders, and how we store such data in secure hospital patient records. Our innovations have included an 'electronic new sheet' to induct staff in Caldicott principles along with computer electronic screen savers. I also hold medical ethics educational sessions for junior doctors and other staff on issues of confidentiality. We are also regularly encouraging staff to complete Caldicott and information governance questionnaires and 'quizzes' to update them on patient confidentiality issues and to ensure that they know who their Caldicott Guardian is!"

Martin is thus trying to 'up the profile' of the Caldicott Guardian and elevate the importance of patient confidentiality within his hospital with the help of the 'Caldicott team'.

The common law duty of confidentiality

74. Common law (or 'case law') is law that has developed through the courts making decisions in cases on legal points and creating binding precedents—in contrast to statutory law, which is determined by acts of parliament. Common law may be used to fill a gap in statutory provision or to interpret what the statute might mean in particular circumstances. There is no statutory provision which sets out a duty of confidence as such, although the DPA provides legal obligations in relation to data sharing.

75. The legal obligation for confidentiality is one of common law, which means it will change as case law evolves. The so-called 'common law duty of confidence' is complex: essentially it means that when someone shares personal information in confidence it must not be disclosed without some form of legal authority or justification. In practice this will often mean that the information cannot be disclosed without that person's explicit consent unless there is another valid legal basis. It is irrelevant whether the individual is old or has mental health issues or indeed lacks capacity: the duty still applies (see also *Information sharing and disclosure: legal considerations* below and the GMC guidance on confidentiality in Annex B).

76. Common law requires there to be a lawful basis for the use or disclosure of personal information that is held in confidence, for example:

- where the individual has capacity and has given valid informed consent;
- where disclosure is in the overriding public interest;
- where there is a statutory basis or legal duty to disclose, e.g. by court order.

Information sharing and disclosure

77. In 2013, Dame Fiona Caldicott's Information Governance Review: information to share or not to share introduced the seventh Caldicott principle: **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 and service users within the framework set out by the Caldicott principles. They should be supported by the policies of their employers, regulators and professional bodies.

78. This seventh principle was designed to encourage teams of professionals providing direct care for a patient or service user to share information across professional or organisational boundaries to maximise safety and quality of care. All health and social care professionals have a responsibility to protect and maintain confidentiality, but they must also be aware of situations where other considerations (such as safeguarding) take precedence and override the duty of confidence.

79. There is a complex legislative framework including common law, statute and case law that covers this area, and there may be differing legal opinion on how the law should be interpreted and applied in individual cases. The role of the Caldicott Guardian is to advise on the ethical as well as the legal considerations, following the Caldicott principles.

80. Whilst the DPA only applies to living individuals, the Caldicott principles also apply to records and information regarding the deceased. The *Access to Health Records* Act gives certain individuals formal rights to access the medical records of the deceased: there is no comparable legislation permitting access to their social care records, although the Caldicott principles may still be applied. After a bereavement, loved ones may have a need for information to help their grieving process and Caldicott Guardians should ensure that appropriate information is not unnecessarily withheld.

Legal considerations

81. Personal information may be shared legally in one of three ways:

- with the consent of the individual concerned (providing that individual has mental capacity: see Annex C);
- when it is required by law (e.g. The Children's Act 1989 requires information to be shared in safeguarding cases);
- when it is in the public interest.

Faouzi Alam is Caldicott Guardian for Cheshire and Wirral Partnership NHS Foundation Trust, which provides care across a wide catchment area for people with mental health problems, learning difficulties, eating disorders, and drug & alcohol issues. It also manages community physical health services and primary care for a population of more than one million. Faouzi is a consultant psychiatrist who cares for people who suffer from first episode psychosis. He is also the Trust's medical director and responsible officer.

Faouzi believes that this combination of clinical work and medical management gives added credibility to his Caldicott role, but also poses some challenges not least because of time constraints. He says: "As is the case with many medical directors and nursing directors, the role of a Caldicott Guardian is an add-on. This might seem a disservice to the Caldicott cause, but with the right support it is a great advantage." In Faouzi's case, a close working relationship with the trust's information governance lead, Gill Monteith, provides the teamwork needed for effective implementation of the Caldicott principles.

Together they provide a focal point for the resolution and/or discussion of information governance issues, which include maintaining service users' confidentiality and safeguarding individuals while promoting appropriate information sharing within and outside the Trust. They work with other care providers and linked agencies to enable better sharing of relevant information about patients, in a manner that facilitates joined-up care across institutional boundaries while ensuring that patients' legal rights and the Caldicott principles are maintained. For example, they attend external meetings to arrange system-wide information sharing for the Cheshire Care Record, a summary record of GP information and several local trusts' information. Gill produces information sharing agreements and checks those received, prior to formal sign off by Faouzi.

They have regular monthly meetings to ensure implementation of Caldicott 2 and to devise action plans for implementation of the EU's new General Data Protection Regulation and the National Data Guardian's recommend-dations. They discuss specific cases, for example breaches of confidentiality and the approach to be taken. They ensure the approach to information handling is communicated to all staff.

Faouzi sees education as key to promoting the Caldicott function; he provides teaching to new recruits and a session for junior doctors at each induction. He also works to develop the information sharing needed to establish a "triangle of care" by involving carers more fully in interactions between patients and professionals.

Faouzi devotes at least half an hour a day to the role of Caldicott Guardian. He says that working as Caldicott Guardian in a mainly mental health trust brings some interesting challenges, especially around issues of mental capacity and information sharing. It is well understood that every patient is presumed to have capacity unless proven otherwise. However, complexities may arise when patients with severe mental illness, learning difficulties, lack of capacity, and a complicated family life are detained in hospital with significant risk issues. Clinicians may have to take very difficult decisions about sharing the necessary information, justifying the purpose, giving access to the right people to view sensitive data and complying with the law — all at the same time.

Faouzi is a member of the UK Caldicott Guardian Council. He always champions mental health issues and brings a psychiatrist's perspective when the council discusses difficult cases requiring an expert opinion.

82. When information sharing is legally permitted, the Caldicott Guardian may need to decide how much information it is appropriate to share, in line with the third Caldicott principle. An organisation may hold a great deal of sensitive information, and any decision to share information must be proportional and relevant.

83. Caldicott Guardians may on occasions be asked to advise on disclosures that may be in the public interest, for example to protect individuals or society from risks of serious harm, such as serious communicable diseases or serious crime, or to enable medical research, education or other secondary uses of information that may ultimately benefit society. Personal information may be disclosed in the public interest, without consent— and in exceptional cases where consent has been withheld— if the benefits to an individual or to society of the disclosure outweigh both the public and the patient's interest in keeping the information confidential.

84. There may be occasions when information sharing is legally permitted but not required. In these circumstances there must still be a justifiable legal basis for breaching confidentiality such as consent, benefit to someone without capacity to consent, or in the public interest.

85. There may also be circumstances where although it is legally permissible to share information, the Caldicott Guardian may decide that it should *not* be shared. There may also be occasions when there is no clear legal basis, or the legal basis is disputed, when the Caldicott Guardian may nevertheless agree that information *may* be shared. The particular circumstances should always be considered in each case, as factors present in one may be absent in another. In all cases, the Caldicott Guardian should be able to justify their decision and provide evidence of their considerations in making the decision.

Quality assurance

86. The Caldicott Guardian also has a potential role in quality assurance of information sharing, for example when a new personal data sharing system is being created. This may require privacy impact assessments, information sharing agreements and protocols, and systems for consent— in all of which matters the Caldicott Guardian can provide independent advice. This in turn may lead to more fundamental changes in organisations' policies and procedures.

The use of patient information in research

87. Organisations that undertake significant amounts of research involving patients or service users will generally have a research governance function or research office dealing with the mechanics of grant application, consent requirements, research ethics committee approval, etc. Those participating in research will normally give informed consent for participation in the research, but should also be informed about and give consent for the uses to which the information collected about them during the research will be put. Caldicott Guardians should ensure that this happens automatically. They may also be asked to advise in situations where a research may involve the use of personal information *without* consent, for example where consent is impracticable to obtain.

88. Person-identifiable information used for research must comply with the provisions of the Data Protection Act—specifically the second principle: *personal data must be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes*, and should only be used with consent.

Lesley Hutchinson is Caldicott Guardian for the Bath and North East Somerset Local Authority (B&NES) where she is Head of Safeguarding and Quality Assurance for both adults' and children's services. B&NES Council is in a formal partnership with Bath and North East Somerset Clinical Commissioning Group under which there is a significant amount of joint commissioning of adult social care and NHS services for adults and children.

Lesley and her fellow Local Authority commissioners are co-located with colleagues from the CCG in Bath. So for example Lesley sits behind the CCG commissioner responsible for medicines management and next to the CCG commissioner responsible for urgent care. These opportunities for exchange of information and ideas put the B&NES health and social care commissioners among the leaders of the drive across England to achieve greater integration.

Lesley became Caldicott Guardian for local authority adult services in 2009 and took on the Caldicott responsibility for children's services as well when her job expanded in 2014. Most aspects to the role are routine, for example quarterly meeting with colleagues responsible for complaints, data protection and subject access requests to review any breaches and all near misses. At the meeting the group also considers the need for staff training and next steps needed to work towards achieving full compliance with the Council's annual self-assessment of strengths and weaknesses when it completes the Information Governance Toolkit.

Lesley and colleagues are also informed of breaches and near misses that occur in commissioned services. One recent case involved a concern that a provider agency was holding service user data on a memory stick and how this was being stored. The Council and CCG have built in reporting these situations to their contract reporting mechanisms.

The Caldicott Guardian is also required to give advice from time to time issues which do not produce a straightforward outcome because of systems and procedural restrictions. For example, whilst staff are aware of the rules and requirements around the secure use of emails and their storage not all agencies have access to secure systems. An example of this is where a foster carer living out of the area may needs to send urgent information electronically about a child to the social work team, the carer will not necessarily have access to the secure emails, and its Lesley's job as Caldicott Guardian to help risk assess the various options and give advice.

Lesley is a member of the Council's Senior Leadership Team. She has a deputy Caldicott Guardian, who is the Complaints and Data Protection Team Manager. There is a page on the staff intranet explaining the Caldicott Guardian role and giving Lesley's email address. There is similar public facing information on the Council's internet site.

89. Whenever possible, person-identifiable information should not be used for research or audit purposes. Research ethics committees now routinely require patient information to be anonymised or pseudonymised. However, particular care should be taken with 'small number data' when even with anonymisation or de-identification it may still be possible to identify individuals.

90. If identifiable information must be used, and consent is genuinely not practicable, then in England and Wales, approval may be obtained from the Secretary of State for Health under Section 251 of the National Health Service Act 2006, on the recommendation of the Confidentiality Advisory Group (CAG) of the Health Research Authority (HRA). CAG[1] provides independent expert advice on the appropriate use of confidential information. It reviews applications for the use of person-identifiable information for research and other secondary purposes, and advises the HRA on whether the use is sufficiently justified. Its key purpose is to protect and promote the interests of patients and the public whilst at the same time facilitating appropriate use of confidential information for purposes beyond direct care.

91. In Scotland, a *Public Benefit and Privacy Panel for Health and Social Care*,[2] which fulfils a similar function to CAG. In Northern Ireland the legislation equivalent to Section 251 is the Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016 (see Annex B). However, as the Act only received Royal Assent in April 2016, at the time of writing none of the sections have yet been commenced, and consequently, in NI there remains no equivalent legal basis to set aside the common law duty of confidence for the time being.

Epilogue

92. It would have been possible to produce a much longer manual with more exhaustive guidance on legal and other matters that Caldicott Guardians may need to address from time to time. However, the UK Caldicott Guardian Council wanted to provide a relatively concise document to assist new and established Caldicott Guardians without overwhelming them.

93. So this manual should be regarded as a starting point in the learning journey. We intend to evolve it over time, and welcome feedback. Annex A is a checklist to help new Caldicott Guardians get up to speed. Annex B lists organisations where Caldicott Guardians can go to obtain help and guidance, as well as some key references for further reading. Annex C provides a brief compendium of key legislation and guidance.

94. The position of Caldicott Guardian can be a lonely one. It often requires wisdom to balance legal and ethical factors, but it may also require independence and resilience. Caldicott Guardians should try whenever possible to support each other. The UK Caldicott Guardian Council has set up regional forums where Caldicott Guardians can meet to share experiences. It also stands ready to debate issues and provide advice when the right answer to a dilemma is by no means obvious.

95. The Council intends to keep this manual up to date by amending the an *online version*[3] to keep abreast of developments. It welcomes *feedback*.[4]

1. CAG succeeds the previous Ethics & Confidentiality Committee of the National Information Governance Board for Health and Social Care (NIGB), and before that the Patient Information Advisory Group (PIAG).
2. http://www.informationgovernance.scot.nhs.uk/pbpphsc/
3. https://www.gov.uk/government/groups/uk-caldicott-guardian-council
4. mailto:ukcgcsecretariat@nhs.net

Annex A—Checklist for new Caldicott Guardians

1. **Have your details been added to the Caldicott Guardian Register?**

   Check the register[1] and contact the *NHS Digital help desk*[2] to update your details if necessary.

2. **Are your details available on your organisation's web site?**

   Search for "Caldicott Guardian" and check your contact details are correct.

3. **Ensure your details are known to organisation switchboard/reception staff.**

   Ring the main switchboard and ask to be put through to the Caldicott Guardian and see what information they provide. Check this is appropriate to ensure you are made aware of these requests. If not, make the necessary changes

4. **Check if there is a generic Caldicott Guardian email address**

   How will you be able to distinguish between your day to day emails and those for your role as Caldicott Guardian? What happens if you are away from the office: will emails be monitored or passed to an appropriate person? How should Caldicott issues be addressed in your absence without a generic email?

5. **Arrange a deputy to cover when you are absent**

   Who will this be? If it is an IG lead are they sufficiently trained to understand your role and how it differs from IG? Will they have access to your Caldicott Guardian mailbox?

6. **Arrange a meeting or meetings with the SIRO and IG leads**

   Use the meetings to gauge the organisation's IG maturity and discuss how you can work together; what support you can offer each other; and your respective roles, responsibilities and expectations.

7. **Information sharing**

   Find out what information sharing agreements (ISAs) and protocols (ISPs) your organisation has, and their reporting/monitoring arrangements. What is the process for approval, and your role involved in approving future agreements? Who checks the organisation is adhering to the agreed protocols? Who are the information asset owners? Are they aware of your role and the need to consult you before sharing information?

8. **Find out how Caldicott decisions are recorded**

   See previous sections on evidence for appraisal, a way of monitoring and evidencing your role and impact is through a decision log.

9. **Establish your accountability and reporting arrangements**

   Who will you report to and what information are you expected to provide? What are the reporting arrangements for information governance generally — for example to the Board? and to whom e.g. input into a quarterly SIRO report at Board level? Many organisations will have an information governance committee or equivalent. Make sure that you are a member of this and your membership is recorded in the committee's terms of reference.

1. https://www.gov.uk/government/groups/uk-caldicott-guardian-council
2. mailto:exeter.helpdesk@hscic.gov.uk

10. Establish your profile

Is there a mention of the Caldicott Guardian role as part of staff induction? Is the role mentioned in the generic data protection training? Plan time out to promote your role with key staff who may need to contact you.

11. Consider what support is available to you

Is there a local or regional network you can join? What events and support are available to you? Sign up to appropriate newsletters e.g. IGA, ICO. Identify peers and perhaps a mentor or coach. See also Annex B: Where to find help and guidance.

12. Understand your IG Toolkit responsibilities

Do you know what you will be expected to sign off annually? Build time in your diary to ensure these tasks are completed before the deadline.

13. Identify your training and development needs

Ensure you have undertaken your SWOT analysis, created your personal development plan, and booked your appraisal in good time. See the section on Learning and Development [page 7].

14. Understand your access to internal audit staff and their reports

Are you notified of any reports which have a Caldicott/IG component? If there is a breach or near miss that requires further investigation and changes in policy/procedure to prevent similar recurrences, are you able to commission any internal audit time to address the issue?

15. Check progress on your organisation's Caldicott2 action plan

Find out how your organisation is progressing against the recommendations in the Caldicott2 report: *Information: to share or not to share.*

16. Compliance

Check your organisation's compliance with the National Data Guardian's *Review of Data Security Consent and Opt Outs* and readiness for the EU General Data Protection Regulation.

Annex B—Where to find help and guidance

Supporting organisations

United Kingdom Caldicott Guardian Council (UKCGC)[1]

The UKCGC is the definitive national body for Caldicott Guardians, providing best practice, advice and guidance, and a bench-mark for all Caldicott Guardians. The Council will also support all professionals across health and care organisations who have a responsibility to implement and uphold the Caldicott principles. It is an independent Council, and a sub-group of the National Data Guardian's Panel.

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

Office of the National Data Guardian

The National Data Guardian for Health and Social Care (NDG) is an independent expert who advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly.

Dame Fiona Caldicott was appointed as the first National Data Guardian by the Secretary of State for Health in November 2014. The role, which is due to be placed on a statutory footing, is to help ensure that the public can trust their confidential information is securely safeguarded, and to make sure that it is used to support citizens' care and to achieve better outcomes from health and care services.

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

Information Governance Alliance (IGA)

The IGA provides a wealth of guidance for both Caldicott Guardians and Senior Information Risk Owners (SIROs). Their newsletters will keep you up to date on IG issues but also on Caldicott Guardian matters. Email them at *iga@nhs.net* to join their mailing list, subscribe to IGA news or to submit an article or showcase an achievement.

https://digital.nhs.uk/information-governance-alliance

NHS Digital

"NHS Digital is the new name for the Health and Social Care Information Centre. We exist to improve health and care by providing information, data and IT services for patients, clinicians, commissioners and researchers."

https://www.digital.nhs.uk/

Professional guidance

General Medical Council – Confidentiality guidance

Confidentiality (2009) sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow. Caldicott Guardians often get asked about the difference between maintaining confidentiality and the duty to share. This guidance helps address this issue. Updated guidance is expected in January 2017.

http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp

General Dental Council

Standards for the dental team sets out six main principles which teams should apply to all aspects of their work as dental professionals.

http://www.gdc-uk.org/Newsandpublications/Publications/Publications/Standards%20for%20the%20Dental%20Team.pdf

British Dental Association

Individual dental practices do not need to appoint their own Caldicott Guardian but they should have appointed

1. Previously known as the UK Council of Caldicott Guardians (UKCCG)

a lead individual (dentist, nurse or other responsible person) for dealing with Caldicott issues. On the BDA website there is guidance around sharing information, primarily around safeguarding.

https://www.bda.org/dentists/advice/Pages/safeguarding.aspx

Nursing and Midwifery Council

Provides guidance on safeguarding, confidentiality, and sharing information with other healthcare professionals.

https://www.nmc.org.uk/

Health and Care Professions Council

Regulating health, psychological and social work professionals. "Our standards of conduct, performance and ethics are the ethical framework within which HCPC registrants must work. It is important that registrants read and understand this document".

http://www.hpc-uk.org/

The Professional Standards Authority (PSA)

"Our policy work covers a broad range of issues across the regulation of health and social care professions. We carry out work when we are asked to look at a particular problem and give our advice. We also identify issues through our work with the professional regulators and accredited registers. The Secretary of State for Health and the health ministers in Northern Ireland, Scotland and Wales often ask us to examine particular questions." The website has a range of guidance including *Sharing Information at First Entry to Registers.*

http://www.professionalstandards.org.uk/what-we-do/improving-regulation/our-policy-advice

Other organisations

Information Commissioner's Office (ICO)

The ICO is: "The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals". It provides a plethora of information and guidance, including model privacy impact assessments and fair processing (privacy) notices.

https://ico.org.uk/

Care Quality Commission (CQC)

The CQC states on its website: "We monitor, inspect and regulate health and social care services. We publish what we find, including ratings to help people choose care". It is expected to incorporate the recommendations from the latest NDG review into its inspection regime, following consultation. The CQC also has responsibility for monitoring IG in the organisations it regulates.

http://www.cqc.org.uk/

Regulation and Quality Improvement Authority

The Northern Ireland counterpart to the Care Quality Commission.

https://www.rqia.org.uk/

Public Health England (PHE)

We protect and improve the nation's health and wellbeing, and reduce health inequalities. PHE provides high quality data and analysis tools and resources for public health professionals.

https://www.gov.uk/government/organisations/public-health-england

Health Research Authority

The HRA protects and promotes the interests of patients and the public in health and social care research. It has developed a single approval process for all study types taking place in the NHS in England. Its *Confidentiality Advisory Group (CAG)* provides independent expert advice on the appropriate use of confidential patient information.

http://www.hra.nhs.uk/

Further reading

To Share or Not to Share. The Information Governance Review

Informally known as *Caldicott2,* this considers how information about patients is shared across the health and care system. It introduced a new Caldicott principle — *Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality.*

It also sets out actions required by Caldicott Guardians in health and social care.

http://ukcgc.uk/docs/caldicott2.pdf

Caldicott2 Implementation Home Page

The information on these pages is intended to assist organisations to implement the recommendations of relevance to them contained in the Caldicott2 Report. It provides information on topics such as monitoring and networks.

https://www.igt.hscic.gov.uk/Caldicott2.aspx

The National Data Guardian's Review of Data Security, Consent and Opt Outs

Published in July 2016, this is the latest report by Dame Fiona Caldicott in her role as the National Data Guardian. The review provides 20 recommendations and 10 data security standards aimed at strengthening the security of health and care information, and ensuring people can make informed choices about how their data is used.

http://ukcgc.uk/docs/caldicott3.pdf

Data security review: letter to NHS Trusts

Just prior to the publication of the review of data security, consent and opt-outs, Dame Fiona Caldicott, the National Data Guardian (NDG), and David Behan, Chief Executive of the CQC, wrote a joint letter to NHS trusts. The letter outlines what trusts should be doing now in the area of data security. This is a succinct aide memoire to check compliance within your organisation, especially if you are subject to CQC audits.

https://www.gov.uk/government/publications/data-security-review-letter-to-nhs-trusts

CQC report Safe data, safe care

Covers how data should be safely and securely managed in the NHS. Makes recommendations *inter alia* on training for Caldicott Guardians and SIROs.

http://www.cqc.org.uk/sites/default/files/20160701%20Data%20security%20review%20FINAL%20for%20web.pdf

Information Governance Toolkit

The IG Toolkit is an online system which allows organisations to assess themselves or be assessed against Information Governance policies and standards. It also makes participating organisations' IG performance available to members of the public.

https://www.igt.hscic.gov.uk/

Information sharing

The Information Commissioner's Office code of practice:

https://ico.org.uk/media/1068/data_sharing_code_of_practice.pdf

Examples of successful information sharing initiatives in Leeds, London and Worcestershire were included in the National Data Guardian's Review of *Data Security, Consent and Opt-Outs* (pages 25-28.).

A series of videos which inform people about how organisations are working together to support those living with dementia:

http://i-network.org.uk/resources/video-library-2/dementia-narratives-multi-agency-working/

Information sharing for secondary purposes in Northern Ireland:

https://www.health-ni.gov.uk/publications/doh-hsc-protocol-sharing-service-user-information-secondary-purposes

Records Management Code of Practice for Health and Social Care

A guide to the practice of managing records based on current legal requirements and best practice. It applies to NHS records, including records of NHS patients treated on behalf of the NHS in the private healthcare sector and public health records, regardless of the media on which they are held. This includes records of staff, complaints, corporate records and any other records held in any format including both paper and digital records. The guidelines also apply to Adult Social Care records where these are integrated with NHS patient records.

http://webarchive.nationalarchives.gov.uk/20160729133355/http:/systems.hscic.gov.uk/infogov/iga/rmcop16718.pdf

Striking the Balance: Guidance on information sharing

This guidance has been published jointly by the Department of Health and the UK Caldicott Guardian Council to assist those who need to share information about individuals involved in domestic violence at a multi-agency risk assessment conference (MARAC) — a local, victim-focused meeting where information is shared on the highest risk cases of domestic abuse between different agencies. It sets out the underlying ethical considerations between confidentiality and information sharing and identifies the role of the Caldicott Guardian in striking the balance between maintaining the individuals' confidentiality and privacy, and wider considerations such as protection from harm.

http://ukcgc.uk/docs/striking-the-balance.pdf

SIRO role and guidance

The NHS has detailed guidance on the SIRO and information asset owner roles. This may help Caldicott Guardians in understanding the differing roles which may be able to assist in the day to day assurance of information risk management:

http://webarchive.nationalarchives.gov.uk/20160729133355/http://systems.hscic.gov.uk/infogov/security/risk

Code of practice on confidential information.

Produced by the HSCIC (now NHS Digital) which has a statutory responsibility under the Health and Social Care Act 2012 to produce a Code of Practice for processing confidential information covering 'the practice to be followed in relation to the collection, analysis, publication and other dissemination of confidential information concerning, or connected with the provision of health services or of adult social care in England.'

http://ukcgc.uk/docs/code.pdf

A guide to confidentiality in health and social care

A practical approach to implementing the HSCIC code of practice above. The second link is to an extensive bibliography:

http://ukcgc.uk/docs/HSCIC-guide-to-confidentiality.pdf

http://ukcgc.uk/docs/confidentiality-guide-references.pdf

The common law duty of confidence

Guidance from Northern Ireland but also more generally applicable:

https://www.health-ni.gov.uk/articles/common-law-duty-confidentiality

Information governance in Scotland

The portal to a comprehensive collection of IG resources.

http://www.informationgovernance.scot.nhs.uk/

NHS Scotland Caldicott Guardians: principles into practice

A foundation manual for Caldicott Guardians in Scotland.

http://www.gov.scot/Resource/Doc/340362/0112733.pdf

The Wales Accord on the Sharing of Personal Information (WASPI)

A framework for organisations concerned with the health, education, safety, and social wellbeing of people in Wales that hold information about individuals, and who need to share that information to deliver effective services.

http://www.waspi.org/

Welsh Health Circular: Duty to Share" and people's access to their electronic care records

Confirms application of the seventh Caldicott principle in Wales.

http://gov.wales/docs/dhss/publications/150409whc013en.pdf

The Centre of Excellence for Information Sharing

Works with a variety of localities across a range of policy areas to help uncover and understand what is limiting good information sharing between them and their partners. A recent information sharing panel debate provides several useful links.

http://informationsharing.org.uk/latestnews/debate/

The risks of absolute medical confidentiality

Explores the concept of patient confidentiality and argues that although a very important medical and bioethical issue, this needs to be wisely delivered to reduce third party harm or even detriment to the patient.

Crook MA (2011) The risks of absolute medical confidentiality. *Science and Engineering Ethics* **19: 107–122.**

Annex C—Key legislation and legal guidance

In addition to the Data Protection Act and common law duty of confidentiality, the most significant items of legislation of which Caldicott Guardians should be aware are listed below. There are others which only assume importance in particular circumstances in which the Caldicott Guardian may occasionally be called upon to offer advice. *The Official Home of UK Legislation.*[1]

Common law

Common law (page 21) exists throughout the UK but the judgements made in one country may not apply to all, although as far as the duty of confidentiality is concerned there are no practical differences. *Common law guidance for Northern Ireland*[2] *Legal guidance on data sharing in Scottish Public Services*.[3]

Human Rights Act 1998

The Human Rights Act 1998 applies to the whole of the UK. effectively brings various rights enshrined in the European Convention of Human Rights into our domestic law. Of particular importance from the Caldicott Guardian perspective, is the impact of Article 8 of the Convention, which is the right which provides for respect for private and family life. This right will be 'engaged' if confidential information about a patient or service user is shared. However, the information sharing will generally not breach the person's rights under Article 8 as long as it is shared lawfully and proportionately (so that the obligations under the DPA and common law have been complied with). An important principle associated with the interpretation of the Act when considering disclosure of confidential information is that of proportionality. *Human Rights Act 1998*.[4] Save the Children has a useful checklist: *Children and the Human Rights Act*.[5]

Mental capacity

The **Mental Capacity Act 2005** provides a legal framework in England and Wales for acting and making decisions on behalf of individuals who lack capacity to make particular decisions for themselves about issues such as their property, financial affairs and health and social care. *Mental Capacity Act.*[6]

The Alzheimer's Society has some useful guidance and flow chart plus links to relevant information for Northern Ireland: *Alzheimer's Society: Mental Capacity.*[7]

The **Adults with Incapacity (Scotland) Act 2000** provides a framework for safeguarding the welfare and managing the finances of adults (people aged 16 or over) who lack capacity due to mental illness, learning disability or a related condition, or an inability to communicate. *Adults with Incapacity Act*.[8]

Mental health

The **Mental Health Act 1983,** significantly updated in 2007, is the law in England and Wales allowing people with a 'mental disorder' to be admitted to hospital, detained and treated, without their consent – either for their own health and safety, or for the protection of other people.

96. A code of practice (2008, updated 2015) shows professionals how to carry out their roles and responsibilities under the Act, to ensure that all patients receive high quality and safe care. *Mental Health Act code of practice*.[9]

97. The **Mental Health (Scotland) Act 2015** is the corresponding legislation for Scotland *Mental Health (Scotland) Act*.[10]

98. In **Northern Ireland** mental health is covered by the *Mental Health (Northern Ireland) Order 1986*.[11]

1. http://www.legislation.gov.uk/
2. https://www.health-ni.gov.uk/articles/common-law-duty-confidentiality
3. http://www.gov.scot/Publications/2004/10/20158/45774
4. http://www.legislation.gov.uk/ukpga/1998/42/schedule/1
5. http://www.savethechildren.org.uk/sites/default/files/docs/Children-and-the-HRA-1998.pdf
6. http://www.legislation.gov.uk/ukpga/2005/9/contents
7. https://www.alzheimers.org.uk/site/scripts/documents_info.php?documentID=354
8. http://www.mwcscot.org.uk/the-law/adults-with-incapacity-act/
9. https://www.gov.uk/government/news/new-mental-health-act-code-of-practice
10. http://www.gov.scot/Topics/Health/Services/Mental-Health/Law/2015Act-provisions
11. http://www.legislation.gov.uk/nisi/1986/595

Section 251 of the NHS Act 2006

Section 251 of the NHS Act applies only in England and Wales. (Corresponding legislation for Scotland and Northern Ireland is described in paragraph 91 above.) It enables the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be legally disclosed. The discloser and applicant must still comply with all other relevant legal obligations e.g. the DPA. It is intended to facilitate essential activities of the NHS and important medical research that require the use of identifiable patient information where it is considered impracticable to obtain patients' consent.

Persons seeking approval for the use of Section 251 must apply to the Confidentiality Advisory Group (CAG) of the Health Research Authority. *Section 251 and the Confidentiality Advisory Group*.[1]

Access to Health Records Act (AHRA) 1990

This applies to the records of deceased patients, for their personal representatives and others having a claim on the deceased's estate. The AHRA is very prescriptive and only permits such access when certain conditions are met. These involve confirming that the person asking for the information is the legal personal representative of the deceased patient. Even where these tests are met this legislation does not grant a general right of access and there are circumstances which could limit disclosure. Guidance is available from the NHS *Guidance for Access to Health Records Requests* ;[2] and the British Medical Association *Access to Health Records*.[3]

Freedom of Information Act

The Freedom of Information Act (FOIA) 2000 and the Freedom of Information Act (Scotland) 2002 are the overarching pieces of primary legislation dealing with information rights. There is a strong interface with the DPA, and with all other legislation which prohibits or limits the disclosure of information in any way. The FOIA also imposes a statutory time limit within which requests must be dealt with (20 working days) and an upper limit applies to disproportionate costs for retrieving and collating information.

The Information Commissioner's Office has provided guidance on the Act in England and Wales: *What is the Freedom of Information Act?*.[4]

The EU General Data Protection Regulation

Notwithstanding the vote to leave the European Union (EU), the EU General Data Protection Regulation will come into force on 25th May 2018. It will affect the following: key definitions of data subjects and personal data; legitimate interests and compatible purposes; consent; data portability; right to erasure/right to be forgotten; data breach notification; data protection by design (privacy impact assessments); data protection Officers, with rights; fair processing; data processors subject to ICO sanctions and enforcement. *ICO Overview of the GDPR*.[5]

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder. Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power but only where it is necessary and expedient for the purposes of the Act. The Home Office has issued guidance on *Information sharing for community safety*.[6]

The Children Act 2004

The Act provides a legislative spine for the wider strategy to improve children's lives. It aims to improve the integrated planning, commissioning and delivery of children's services, promote early intervention, provide strong leadership and bring together different professionals in multi-disciplinary teams in order achieve positive outcomes and improve the well being of children and young people and their families. *Working together to safeguard children*.[7]

The Care Act 2014

Defines local authorities' responsibilities for cooperation with other parties, which is likely to involve information sharing (or protection). *Care Act 2014*.[8]

1. http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/
2. http://www.nhs.uk/chq/Documents/Guidance%20for%20Access%20to%20Health%20Records%20Requests.pdf
3. https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/access-to-health-records
4. https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/
5. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
6. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97842/guidance.pdf
7. https://www.gov.uk/government/publications/working-together-to-safeguard-children--2
8. http://www.legislation.gov.uk/ukpga/2014/23/contents

Other relevant legislation

The Human Fertilisation and Embryology Act 2008 imposes restrictions on the disclosure of specific personal information.

The **Abortion Regulations 1991** provide a statutory gateway for disclosure of certificates of opinion to the Chief Medical Officer as required by the Abortion Act 1967.

The **Gender Recognition (Disclosure of Information)** England, Wales and Northern Ireland (No 2) Order 2005 is gateway legislation which allows disclosure of information to a health professional which is otherwise prohibited by the **Gender Recognition Act 2004.**

The Road Traffic Acts (RTAs) make provision for the disclosure of information by NHS bodies to enable the recovery of any costs of treatment. RTAs also require the NHS to provide any information which it is in their power to give and which may lead to the identification of a driver who has committed an offence under the Acts.

These are the most significant examples of the Acts and common law directly involved in the protection of patient-identifiable information. There are others which only assume importance in particular circumstances in which the Caldicott Guardian may occasionally be called upon to offer advice.

Annex D—Glossary of abbreviations

AHRA	Access to Health Records Act
CAG	The Confidentiality Advisory Group of the Health Research Authority
CCG	Clinical Commissioning Group
CPD	Continuing professional development
CQC	The Care Quality Commission
DPA	The Data Protection Act 1998
EU	European Union
FOIA	Freedom of Information Act
GDPR	The EU General Data Protection Regulation
GP	General practitioner
HRA	The NHS Health Research Authority
HSCIC	The Health and Social Care Information Centre; now NHS Digital
IAO	Information asset owner
ICO	The Information Commissioner's Office
IG	Information governance
IGA	The Information Governance Alliance
IGTK	Information Governance Toolkit
IM&T	Information management and technology
LAC	Local Authority Circular
MARAC	Multi-agency risk assessment conference
NDG	The National Data Guardian for Health and Social Care. Presently Dame Fiona Caldicott
NHS	National Health Service
PHE	Public Health England
PSA	The Professional Standards Agency
SIRO	Senior Information Risk Officer
SWOT	Strengths, weaknesses, opportunities and threats
UKCGC	The United Kingdom Caldicott Guardian Council (previously United Kingdom Council of Caldicott Guardians – UKCCG)
WASPI	The Wales Accord on the Sharing of Personal Information

2905908 Prepared by Williams Lea