The Caldicott Guardian in Health and Social Care

Workbook

Name:

Job role:

Department:

Document Name	Version	Status	Author
The Caldicott Guardian in Health and Social Care Workbook	1.0	Final	Information Governance Services based on previous versions issued by NHS Digital

Document objectives:	This workbook updates a previous version originally issued by NHS Digital. Local amendments to this workbook were recommended by NHS Digital should an organisation wish to continue to use it as there were no plans to do this centrally. It can be used as an additional resource for Caldicott Guardians who can use the assessment included as evidence of continuing learning and development.	
Target audience:	Caldicott Guardians	
Committee/Group Consulted*:*	SCW Information Governance Senior Management Team	
Monitoring arrangements and indicators:	This workbook will be monitored by the Information Governance Team to ensure any legislative changes that occur before the review date are incorporated.	
Training/resource implications:	Caldicott Guardians – the workbook will be shared by staff where an enquiry for training of this type has been received.	
Approved and ratified by:	SCW Information Governance Senior Management Team	Date: 23-11-18
Equality Impact Assessment:	Not required	Date: NA
Date issued:	23-11-2018	
Review date:	November 2019	
Author:	Information Governance Team	
Lead Director:	Head of Information Governance	

Change Record

Date	Author	Version	Page	Reason for Change
Nov 18	Angela Sumner	1.0	Various	Amend due to changes in Data Protection Legislation

Reviewers/contributors

Name	Position	Version Reviewed
Angela Sumner	Senior Information Governance Manager	V1.0
Shelley Brown	Regional Information Governance Lead	V1.0
Kate Tregale	Regional Information Governance Lead	V1.0
Trudy Slade	Information Governance Manager	V1.0

Contents

The Caldicott Guardian in Health and Social Care Workbook 5

Description 5

Learning Objectives 5

Introduction 5

The Caldicott Guardian: a senior role 6

The introduction of Caldicott Guardians 6

The Caldicott Principles 6

UK Caldicott Guardian Council 7

The National Data Guardian 8

Qualities of a Guardian 8

Seniority of the Caldicott Guardian role 9

Summary 10

Working with the Senior Information Risk Owner 10

The Senior Information Risk Owner (SIRO) 10

The distinction between the roles 11

Working with the Data Protection Officer 12

The Data Protection Officer (DPO) 12

Expertise and skills of the DPO 12

The distinction between the roles 13

Information mapping 14

Managing an incident 14

Working with others - Summary 14

Information Governance 15

Annual governance statement 15

Audit 15

Summary ... 16
Responsibilities of the role ... 16
Strategic role ... 17
Advisory role ... 18
Operational role ... 18
Working strategically ... 19
Summary ... 23
Relevant law and guidance ... 23
The Data Protection Act 2018 ... 24
The General Data Protection Regulation ... 25
Other relevant legislation ... 32
Summary ... 33
Applying law and guidance ... 33
Scenario 1: Internal information processing ... 34
Scenario 2: Sharing information in the public interest ... 35
Scenario 3: Disclosure to assist a criminal investigation ... 37
Scenario 4: In a different light ... 39
Scenario 5: Subject access request under the Right of Access ... 40
Scenario 6: Access to records of the deceased ... 41
Scenario 7: Sharing non-confidential personal information without consent ... 43
Scenario 8: Access to confidential patient information for clinical audit ... 45
Resources for Caldicott Guardians ... 46
Guidance and websites ... 47
Answers to Knowledge check questions ... 48
Assessment ... 52

The Caldicott Guardian in Health and Social Care Workbook

Description

What does the Caldicott Guardian do, and who can help them in their role? This workbook will answer these and other questions such as why the role should be allocated to a senior member of staff and how it fits into the wider Information Governance Assurance framework. The material is designed to assist Guardians to arrive at lawful and practical decisions regarding the protection and sharing of patient and service user information. It should be read alongside ‘’: A Manual for Caldicott Guardians.

The learning includes an assessment at the end. You should give the completed assessment to your IG lead so your responses can be reviewed and logged.

Compiler: NHS Digital (External IG Delivery) updated by SCW IG team in response to changes in Data Protection Legislation.

Duration: Approx. 1 hour

Learning Objectives

By the end of this workbook you will understand:

- How and why the senior role of Caldicott Guardian was created.
- The importance of the Caldicott Principles in making balanced judgements for your organisation.
- The role of the UK Caldicott Guardian Council.
- The relationship between the Guardian and the Senior Information Risk Owner (SIRO) and the Data Protection Officer (DPO).
- How Caldicott Guardianship fits within broader Information Governance.
- The responsibilities and duties of a Caldicott Guardian.
- How to apply the relevant law and guidance to some common situations.
- Where to find resources that will help you in your role.

Introduction

This is a practitioner level module based on materials published by the UK Caldicott Guardian Council and the Information Governance Alliance, which is designed to provide information about the role of the Caldicott Guardian and advice about dealing with Caldicott and confidentiality issues.

It is aimed at newly appointed Caldicott Guardians and those needing to know more about the role of the Caldicott Guardian. It may also be useful as a refresher session for more experienced Caldicott Guardians.

The Caldicott Guardian: a senior role

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

The introduction of Caldicott Guardians

Caldicott Guardians derive their name and inspiration from the 'Report of the Review of Patient-Identifiable Information', Caldicott 1 chaired by Dame Fiona Caldicott, which reported in December 1997. The Caldicott Committee made 16 recommendations to improve the security and confidentiality of patient identifiable information. One of the 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 appointment of a Caldicott Guardian was mandated for the NHS by a Health Service Circular: HSC 1999/012 and was subsequently introduced into Social Care in 2002, mandated by Local Authority Circular: LAC 2002/2. Since the mandates, all NHS organisations and local authorities providing social services must have a Caldicott Guardian, who must be registered on the publicly available Caldicott Guardian Register. Other health and care organisations (e.g. from the independent sector) are encouraged to register a Caldicott Guardian.

All organisations which are required to have a Caldicott Guardian should ensure their up-to-date details are on the Caldicott Guardian Register, available on the NHS Digital website. If the Caldicott Guardian's details need adding or amending, a registration form is also available for download from the same web page.

The Caldicott Principles

The 'Report on the Review of Patient-Identifiable Information' also set out six principles for determining when confidential information might be used and when it should not. In 2013, Dame Fiona completed her 2nd Information Governance Review Caldicott 2 and introduced a 7th principle.

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.

UK Caldicott Guardian Council

The UK Council of Caldicott Guardians was established in 2005 as an elected body comprised of Guardians from the health and social care communities. The Council, now called the UK Caldicott Guardian Council, is the national body for Caldicott Guardians and is a sub-group of the National Data Guardian's Panel.

The Council has developed 'A Manual for Caldicott Guardians 2017', which offers 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.

The Manual can be downloaded from the Council's website at: UK Caldicott Guardian Council.

As part of their role, the Council provides advice on the resolution of Caldicott queries. If you would like to find out more about the Council or seek their advice, you can contact the Secretariat at ukcgcsecretariat@nhs.net.

The National Data Guardian

Dame Fiona Caldicott is the first National Data Guardian (NDG). The role advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly. The NDG Panel is an independent group of experts that advise and support this work. The Panel is guided by three main principles:

- Encouraging clinicians and other members of care teams to share information to enable joined-up care, better diagnosis and treatment.
- Ensuring there are no surprises to the citizen about how their health and care data is being used and that they are given a choice about this.
- Building a dialogue with the public about how we all wish information to be used.

A 3rd Caldicott report Review of Data Security, Consent and Opt-Outs carried out in 2016 by the National Data Guardian reaffirmed the importance of the Caldicott Principles. The review sets out three Leadership Obligations and ten Data Security Standards that are applicable to all health and care organisations.

You can find out more on the NDG website at: National Data Guardian.

Qualities of a Guardian

Experience

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 and service user information.

The Caldicott Guardian role is a strategic one that requires someone with sufficient experience and seniority to represent and champion confidentiality issues at Board / senior management team 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.

The Caldicott Guardian needs excellent influencing skills to be able to direct confidentiality policy within their organisation. Where necessary, they should be comfortable challenging established practice and be able to clearly explain the rationale for their decisions.

Knowledge

Operationally, the Guardian must be able to show that they understand how confidential patient/service user information is used in the organisation, and have an understanding of the information sharing requirements of internal staff and external organisations.

They must be able to instil confidence in their colleagues by making justifiable and practical decisions about uses of confidential personal information. Therefore, the appointed person needs to be very familiar with key influential guidance and legislation such as the common law duty of confidence and the Data Protection Legislation.

Knowledge Check - Qualities of a Guardian

Which of the following knowledge and experiences are you likely to need to carry out the role? Tick **two or more options** from the answers listed below; then go to knowledge check to check your answer.		
A	Extensive knowledge of legal issues	
B	Knowledge of how information is used and shared	
C	Experience of drafting Information Governance policies	
D	Experience of working at a senior level	

Seniority of the Caldicott Guardian role

It is recommended that a Caldicott Guardian should be (in order of priority):

- An existing member of the Board or senior management team.
- A senior health or social care professional within the organisation.
- The person responsible for promoting clinical governance or an equivalent function within the organisation.

Not all Caldicott Guardians are 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 who are experts 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 general practices, pharmacies and charities.

Knowledge Check - Who should be the Caldicott Guardian?

Appointing a suitable person to be a Caldicott Guardian is vital. Have a look at this situation and then, when you're clear on the details, move to the next page to answer a question about it.

Jennifer is the IG lead in a local authority. She has been in post for a year and before that worked as a social worker in the same organisation. The Caldicott Guardian has recently resigned and Jennifer has been asked to compile a briefing paper for her line manager, the Assistant Head of Corporate Services, to present to the senior management team. The paper should set out the type of person that should be the next Caldicott Guardian.

Based on the scenario, would Jennifer be justified in recommending that she takes on the role of Caldicott Guardian herself? Tick one of the options below, and then go to Knowledge check to check your answer.

A.	Yes	
B.	No	

Summary

The importance of the role of Caldicott Guardian requires that people who hold this post are:

- Senior figures within their organisation already working at senior management level.
- People with a clear grasp of the issues affecting confidentiality and consent.
- Aware of the legislation and guidance that supports confidentiality and consent issues.
- Able to make practical decisions that help the organisation to respond effectively to confidentiality issues.

Working with the Senior Information Risk Owner

The Senior Information Risk Owner (SIRO)

The Cabinet Office Data Handling Review in 2008 led to a requirement for NHS organisations and local authorities (as public sector bodies) to assign the role of the Senior Information Risk Owner (SIRO), a board level executive with particular responsibility for information risk.

The SIRO has responsibility for understanding how the strategic business goals of the organisation may be impacted by any information risks and for taking steps to mitigate those risks. As part of the management of information risks, organisations are required to carry out work to identify their information assets and assign "ownership" for each asset to an Information Asset Owner (IAO). The IAO should be a senior member of staff who is accountable to the SIRO.

The distinction between the roles

A Caldicott Guardian's 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.

At the same time there is a clear need to ensure that the Caldicott Guardian works closely with the SIRO (and any IAOs) and that the Guardian is appropriately consulted when information risk reviews are conducted for assets which are or that contain personal information.

Knowledge Check - Working with the SIRO

The role of SIRO is distinct from the role of the Caldicott Guardian, which of the following are part of the SIRO role? Tick **two or more options** from the answers listed below, and then go to Knowledge check to check your answer.		
A	Providing organisational direction for data handling and information risk management	
B	A point of contact for information incidents	
C	Providing an advisory service to the organisation	
D	Ensuring that patient/service user information is used to provide effective care	

Distinct but complementary

The roles are distinct but complementary - Consider the following scenario which illustrates the different roles.

Your organisation receives a request for patient/service user information from the Care Quality Commission (CQC). Your advice is sought on whether the information can be disclosed and if so, whether the method of transfer suggested by the monitoring body is appropriate.

In this situation you as Caldicott Guardian should give advice on whether it would be appropriate to disclose the requested information.

However, you should seek advice from the SIRO / IAO on transferring the information by the suggested method to ensure that any and all risks are taken into account.

On some projects the boundaries will be blurred and Caldicott Guardian and SIRO will work more closely together as well as with others. For example, understanding what information is used in an organisation, and responding to any information incidents will involve the Guardian, the SIRO and the new Data Protection Officer role. Their roles won't be the same and they won't work in isolation.

Can you be a Caldicott Guardian and a SIRO?
Due to the distinct nature of the roles and to prevent any possible conflict of interests the two roles should not be held by one person.

Working with the Data Protection Officer

The Data Protection Officer (DPO)

- The role of the DPO includes the following key responsibilities:
- Inform and advise the organisation of their obligations under the Data Protection Legislation
- Act as the contact for data subjects with regard to all issues related to processing of their personal data and to the exercise of their rights under Data Protection Legislation
- Act as a contact point for the supervisory authority (ICO) on all Data Protection issues
- Working with the SIRO, understand the risks associated with the nature, scope, context and purposes of processing for the organisation
- Advise which areas should be subject to an internal or external data protection audit
- Advise on the internal training activities to provide to staff or management
- Monitoring compliance with the GDPR
- Provide support and advice on the preparation of a data protection impact assessment and monitor its performance
- Provide support and advice on the maintenance of records of processing operations under its responsibility' or 'maintain a record of all categories of processing activities carried out on behalf of a controller'

Expertise and skills of the DPO

- The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the DPO tasks

- Be able to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned
- The DPO should also have a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the health sector
- The DPO should have a sound knowledge of the administrative rules and procedures of the organisation
- Report directly to the highest level of management and work independently to perform their tasks
- Ensure that any other tasks or duties they undertake do not result in a conflict of interests

The distinction between the roles

Knowledge Check - Working with the DPO

The role of DPO is distinct from the role of the Caldicott Guardian, which of the following are part of the DPO role? Tick **two or more options** from the answers listed below, and then go to Knowledge check to check your answer.		
A	Ensuring the organisation undertakes all of the necessary compliance and assurance checks required for the IG toolkit	
B	A point of contact for information incidents with the Information Commissioners Office	
C	Providing an advisory service to the organisation	
D	Ensuring that patient/service user information is used according to Data Protection Legislation	

Distinct but complementary

The roles are distinct but complementary - Consider the following scenario which illustrates the different roles.

Following a Data Protection Breach, the Information Commissioners Office require an action plan to be put in place to address the failings found during the investigation into the breach. The action plan requires the organisation to a) source appropriate and up to date Information Governance training for all staff across the organisation, b) ensure that a register of assets is put in place and owners identified for each asset and c) all fax machines in use across the organisation are replaced with a more secure method of sharing Personal Data that is deemed to be confidential.

The DPO will take the lead on developing the action plan, will work with the SIRO to ensure that any resultant risks to the organization that are either financial or reputational are documented and managed. Both the DPO and the SIRO will work

with the Guardian to ensure that the proposed actions meet confidentiality obligations.

Can you be a Caldicott Guardian and a DPO?
Due to the distinct nature of the roles and to prevent any possible conflict of interests the two roles should not be held by one person.

Information mapping

Organisations are required to ensure they have identified (or mapped) all the personal information they have, with the aim of ensuring information:

- Is protected at all points during its use, and
- Is only used when there is a legal basis to do so.

The process involves documenting categories of information, their transfer from one physical location to another and the method by which the information is transferred. The work should be overseen by both the Caldicott Guardian and the SIRO but will probably be led by the DPO; it should involve managers from each area of the organisation.

Managing an incident

If there is a breach of the Data Protection Legislation or the common law duty of confidentiality, the Caldicott Guardian must be made aware.

The role of the DPO would be to lead on the response and management of such an incident, including the reporting of serious incidents requiring investigation (SIRIs) and near-misses and any necessary communication with the Information Commissioners Office (ICO).

Depending on how the breach occurred, the Guardian and the SIRO should be involved in any review of confidentiality and information sharing procedures as part of the 'lessons learned' process.

Working with others - Summary

The roles of Caldicott Guardian and SIRO are important in ensuring the effective management of information in an organisation alongside the DPO. As a Caldicott Guardian you need to:

- Be consulted when any information risk reviews concerning personal information are carried out.
- Be aware of any confidentiality issues related to the SIRO's information risk work.

- Work with the DPO and SIRO on issues that cross responsibility areas, e.g. information mapping.
- Coordinate your work and the organisation's response, together with that of the DPO and the SIRO, if there is an incident affecting personal information.

There is more on the role of the SIRO, in the Introduction to Risk Management for SIROs and IAOs workbook.

Information Governance

Information governance is a broad framework for ensuring and assuring that information is managed legally, securely, efficiently and effectively in order to support delivery of the best possible care. This includes appropriate internal measures (people, process and technology) and external oversight (monitoring and audit).
Organisations are required to demonstrate they are complying with the law and national guidance when using personal information. Health and care organisations use a centrally provided tool to measure their compliance.

As Caldicott Guardian, you should work closely with the DPO, IG staff and others acting in an advisory role to ensure that there are robust confidentiality and data protection arrangements and staff guidance in place regarding *who* should be able to access personal information. You should also support IG staff in monitoring/checking compliance with the confidentiality and data protection arrangements.

Annual governance statement

Most health and care organisations are required to, or choose to publish annual governance statements that:

- Describe how the organisation manages risks and includes how risks to personal information are managed and controlled.
- Explicitly includes disclosure of any serious incidents relating to personal information including data loss or confidentiality breach.

As Caldicott Guardian, you should keep your Board/senior management team up to date with confidentiality issues and support the reporting of data protection matters (e.g. new processes, new information sharing, new protective measures) by the DPO, so that where appropriate, they can be included within the organisation's governance statement.

Audit

Information governance should be considered as part of the risk management regime and be formally audited. It might be reviewed by the organisation's audit committee or equivalent, or there might be an external audit carried out by an

independent 3rd party. In either case you should ensure the Board/senior management team are:

- Appropriately briefed by the DPO on the audit report results relating to confidentiality and data protection, including being made aware of areas of concern and any resultant implications.
- Presented with options for improvement including, where necessary, a confidentiality strategy to implement any improvements in support of the DPO.

Knowledge Check - Information Governance

How does your role support the wider information governance agenda? Tick **two or more options** from the answers listed below, and then go to Knowledge check to check your answer.		
A	Ensuring the Board is fully informed of any confidentiality concerns	
B	Ensuring the arrangements for confidentiality and data protection are monitored by the DPO	
C	Carrying out internal audits relating to confidentiality and data protection assurance	
D	Arranging external auditors to carry out confidentiality and data protection assurance audits	

Summary

With the increasingly raised profile of Information Governance and data security, the Caldicott Guardian has a role to play in making sure that information governance is properly embedded into the organisation. In particular this means that you should:

- Support confidentiality and data protection issues and ensure that they are properly reported to and discussed at Board/senior management team level.
- Advise the Board/senior management team on the inclusion of confidentiality matters into annual governance statements.
- Support the DPO in ensuring that results of internal and external audits are discussed at Board/senior management team level.

As a Caldicott Guardian, you are vital to ensuring that the Board/senior management team are kept informed and up-to-date by the DPO, so that they appreciate the necessity for confidentiality and data protection assurance and recognise there is a real impact on real people if things go wrong.

Responsibilities of the role

The Caldicott Guardian should act as the conscience of the organisation, ensuring that both legal and ethical considerations are taken into account, particularly when deciding whether to share confidential information.

The responsibilities fall into three main categories:

1. Strategic role.
2. Advisory role.
3. Operational role.

Strategic role

The strategic role covers both governance and the promoting of an appropriate culture within the organisation.

Strategy and governance

As well as being a champion for information sharing and confidentiality issues at Board/senior management team level the Caldicott Guardian should sit on an organisation's Information Governance Steering Group or equivalent forum.
As part of their strategic role the Guardian needs to be familiar with the organisation's business and goals, particularly in relation to the use and sharing of confidential information.

You must be able to support the DPO and help to advise the Board/senior management team of current information sharing and confidentiality working practices within the organisation, and whether these are in line with the organisation's overall business strategy.

Promoting appropriate information sharing within a confidentiality culture

Caldicott Guardians should provide regular reports to the Board/senior management team which include measures to promote the sharing of information when it is appropriate to do so, within a culture of confidentiality. The basis of your reports should cover such matters as:

- The number and type of Caldicott issues that have been logged since the previous report.
- The number of issues that have been satisfactorily resolved.
- The number and type of issues that are still pending and the reason that they have not been resolved.
- Any issues that have been escalated due to an unsatisfactory response from the organisation, or because the issue has become more pressing and requires a more immediate response.

Your reports should include clear indication of any necessary improvements, addressing issues such as the implementation of a new policy or procedure, the need for staff training and awareness, etc. In addition, required operational resources for implementation (human, financial or time allocated to the role) should also be included.

Advisory role

The Caldicott Guardian's advisory role involves not only providing day to day advice on information sharing and confidentiality issues but also being an arbiter when there is disagreement about a process potentially impacting on information sharing or confidentiality.

Providing information sharing and confidentiality advice

The Caldicott Guardian should be a contact point for the Board/senior management team and employees on lawful processing of information, in accordance with the Data Protection Legislation and the common law duty of confidentiality.

Although you should have a good knowledge of information sharing and confidentiality matters, you should access internal and external sources of advice and guidance. The DPO for your organisation will be able to assist you with this.

Issue resolution

The Caldicott Guardian should help to resolve local issues impacting on the information sharing and confidentiality agenda. It is recommended that Guardians keep a record of resolved Caldicott issues. This should detail the issue, the decision taken and the time/resources taken to resolve the issue.

You will find these records useful should a similar issue be raised in future, and also as evidence when making the case for adequate time or resource to carry out the role.

Operational role

The Caldicott Guardian's operational role is concerned with how information is processed within the organisation and with whom it is shared outside the organisation. This includes keeping up to date with the types of personal information used in the organisation and being aware of the staff groups that have access to it.

Internal information processing

The Caldicott Guardian plays a key role in ensuring the organisation satisfies the highest practical standards for handling personal information. Working with the DPO and operational staff, you should ensure that the rules on information sharing and confidentiality are appropriately reflected in organisational strategies, policies and working procedures.

The role also includes:

- Supporting information sharing and confidentiality training being included within the organisation's overall training strategy; and
- If there has been a confidentiality incident, ensuring there is an appropriate process to disseminate lessons learned to staff.

Information sharing

The Caldicott Guardian should actively support work to facilitate and enable appropriate information sharing, ensuring that processes are in place to ensure that legal requirements are met. You should oversee arrangements, protocols and procedures where confidential patient / service user information may be shared both inside, and outside the organisation. For example, flows of information to and from partner agencies, sharing through nationally provided IT systems, disclosure to research interests, and disclosure to the police.

These operational responsibilities do not mean that you must draft the strategies, policies and protocols etc. yourself, but it does mean that you are a key contributor to the approval process where there is a need to share personal information.

Knowledge Check - Responsibilities of the role

How can the Caldicott Guardian help to ensure that confidentiality is embedded into the organisation? Tick **two or more options** from the answers listed below, and then go to Knowledge check to check your answer.		
A	Ensuring the Board/senior management team are adequately informed about confidentiality issues	
B	Ensuring that confidential information is not shared for clinical/care purposes	
C	Ensuring staff are provided with clear guidelines and procedures	
D	Ensuring that identified improvements to confidentiality processes are implemented	

Working strategically

Partnerships, particularly with organisations outside the NHS or adult social care may raise complex issues that will require an opinion from a Caldicott Guardian. Consider the following scenario then read on to look at some of the issues that need to be taken into account.

Your Trust is considering a partnership with a private company that will offer day care surgery from a new building in the hospital grounds.

The facility will treat direct access private patients (e.g. insurance scheme referrals) and NHS referrals from the Trust. The Trust proposes to extend its patient administration system to the new facility.

Although the private facility will maintain separate health records, it will effectively be set up as an additional ward with requests for records and x-rays treated as if they originated in the Trust. The Board has asked for your opinion on the proposal in relation to any confidentiality concerns.

The duty to share

You should consider the Health and Social Care (Safety and Quality) Act 2015, which introduced a legal duty requiring health and adult social care bodies to share information where this will facilitate care for an individual. The Act reinforces existing good practice and obligations on health and social care professionals and provides statutory support for the seventh Caldicott principle that:

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

It makes it clear that unless an individual objects, when information can be lawfully shared between health or adult social care commissioners or providers for purposes likely to facilitate the provision of health services or adult social care and are in an individual's best interests, then it must be shared.

You will need to consider whether information can be lawfully shared and whether it will facilitate the provision of health services and adult social care.

The common law duty of confidentiality

In considering whether the information can be lawfully shared, you should assess whether the proposal would breach the common law duty of confidentiality. Patients directly accessing private care may have informed the clinicians of their past medical history and **might** expect information about this to be obtained from the NHS.

However, there may also be patients that have specifically chosen to go private so that they are treated without reference to their past medical history.

Processes in the new facility

To ensure all patients are treated consistently and that there are "no surprises", communications materials provided to patients of the new facility should be transparent and should clearly set out the working relationship with the NHS Trust. Materials should explicitly state that, where relevant and available, information about the patient will be obtained from the Trust.

Staff of the new facility should check that patients have understood the information leaflet and are aware of their choices in respect of information sharing. Processes

will need to be put in place for patients that refuse their consent (for the private facility to access their NHS records) to ensure that their wishes are complied with.

Processes in the Trust

Similarly, just because the private facility is being treated as an additional ward for administration purposes, this does not give the Trust the right to access private patient health records without consent. Explicit patient consent would be required before the Trust accesses the private health records of its NHS patients.

Internal procedures and access controls

Another consideration you need to make is whether the proposal is in line with the organisation's confidentiality strategy. For example, do current procedures advise staff about inappropriate access to records and are there measures to ensure only authorised employees are able to access patient information?

Are the measures sufficiently robust so that only those who need to know as part of their job role, whether in the Trust or the new facility, will have access to the appropriate records? Are there any improvements that can be made e.g. regular checking and monitoring of system audit trails to see who has done what with a patient record? Are additional resources required, e.g. to manage the audit process?

Additionally, there will need to be clear procedures for staff in health records departments setting out when private patient records can be released to the Trust and vice versa.

Contracts of employment and third parties

Another consideration would relate to the contractual status of the workers in the new facility. Will they be employees of the Trust and therefore be subject to the same contractual obligations as all other Trust employees? Or will they be categorised as third party contractors, in which case additional provisions might be applied? The Board will take advice from a range of other staff in the Trust in relation to contracts and information governance.

Staff also need to be made aware of their obligations regarding confidentiality, and that breach of confidence, inappropriate use of patient records, or abuse of computer systems may lead to disciplinary measures, bring into question professional registration and possibly result in legal proceedings.

Your role as Caldicott Guardian, is to reinforce the necessity for all staff (either of the new facility or the Trust) to have confidentiality requirements clearly stated in their contracts, and to ensure there is a process in place by which staff are informed of their confidentiality obligations.

National IT Infrastructure

A number of the access controls issues mentioned in the scenario will be addressed by the controls built into the national IT systems that NHS Digital develops, delivers and maintains to support the provision of health and care services in England. These systems help to manage day-to-day operations and improve the quality of patient / service user care.

Some of the systems are:

- Summary Care Records
- NHS e-Referral Service
- Spine
- Electronic Prescription Service
- GP2GP
- NHS Wi-Fi
- NHSmail

Information governance is central to all of these systems to ensure security, confidentiality, fair processing and quality of information. Information governance is enhanced by a number of measures, for example, registration authorities, smartcards and the proactive review of audit logs and monitoring of alerts. There is more information about these systems and the access control mechanisms on the NHS Digital website: NHS Digital systems and access.

Knowledge Check: Sharing demographic information

You receive a request for information from the police. They are investigating a missing person case and want your organisation to supply contact details of any recipient of services called John Smith. You are informed that there are five 'John Smiths' listed as service users.

If you supply the information as requested, have you breached the Caldicott Principles? Tick one of the options below, and then go to Knowledge check to check your answer.

A.	No. It's an important request from the police and the information should be supplied	
B.	No. The police are not asking for clinical/care information so this information can be supplied	
C.	Yes. The police are not asking for clinical/care information but even so the information should not be supplied	
D.	Yes. But it's an important request from the police and if it helps to locate the person it is in the public interest	

Summary

Your role and responsibilities as Caldicott Guardian are comprised of strategic, advisory and operational aspects to ensure patient / service user information is used and shared appropriately, and their confidentiality is respected and maintained. They include the following:

- Strategic: you should be aware of how procedures for processing confidential information might impact on the organisation's business and goals; and champion confidentiality issues at Board/senior management team level.
- Strategic: you should promote a culture of appropriate information sharing and confidentiality by making sure the organisation upholds the highest standards and best practice.
- Advisory: you should develop a strong knowledge of information sharing, confidentiality and data protection matters, so that you can advise staff on the issues.
- Advisory: you should contribute to the resolution of local issues that impact on the information sharing and confidentiality agenda, keeping a log of Caldicott issues to assist with similar queries.
- Operational: you should ensure that information sharing and confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff; and ensure that staff have access to appropriate training.
- Operational: you should oversee all arrangements, protocols and procedures where confidential personal information may be shared with external bodies and others with responsibilities for health or social care and safeguarding.

Relevant law and guidance

The Caldicott Guardian needs of course to be familiar with the Caldicott Principles but they should also be aware of the Data Protection legislation that governs how organisations must safeguard information, what processes should be in place to use, secure and transfer information and also how patients and members of public can exercise their rights under that legislation. This area is complex but can be viewed as follows.

Data Protection Legislation can be used as a generic term which encompasses the following:

- the Data Protection Act 2018 (DPA 2018)
- the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679),
- the Law Enforcement Directive (LED) (Directive (EU) 2016/680)
- regulations made under the DPA 2018
- any applicable national Laws implementing them as amended from time to time

- all applicable Law concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations

In addition, organisations must take account of the following as part of their information governance and management practices:

- Freedom of Information Act 2000
- Environmental Information Regulations
- INSPIRE Regulations
- Health and Social Care Act 2012
- Access to Health Records Act 1990
- Public Records Act 1958
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988

An organisation must also have regard for the following standards and Codes of Practice where these are relevant to them:

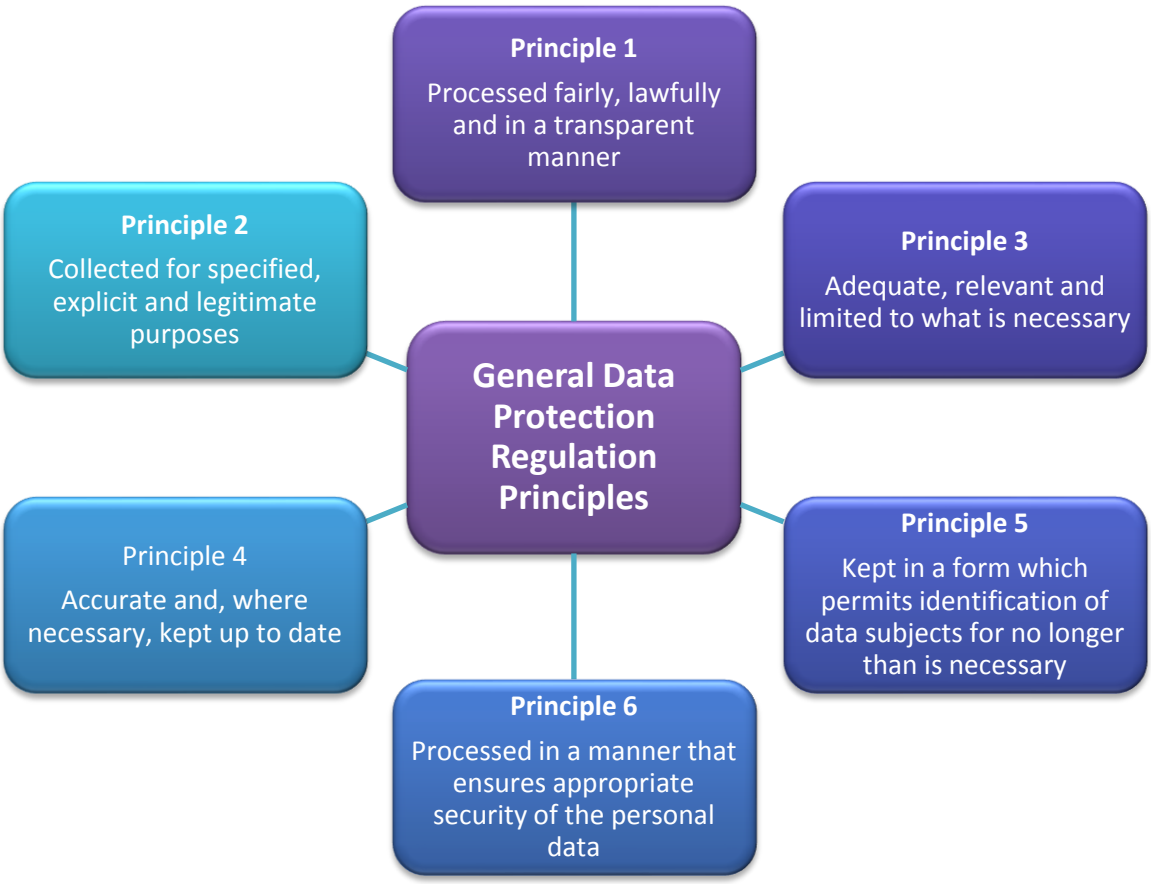
- International information security standard: ISO/IEC 27002: 2005
- Caldicott Principles
- Data Security and Protection Toolkit
- Data and cyber security: protecting information and data in health and care
- Data Sharing - Data Protection Code of Practice - ICO
- Codes of practice for handling information in health and care
    - Records Management Code of Practice for Health and Social Care
    - Code of practice on confidential information
    - HSCIC Guide to Confidentiality
    - Confidentiality
    - Information security management NHS code of practice
    - NHS Information Governance - Guidance on Legal and Professional Obligations
- Confidentiality Supplementary Guidance - Public interest disclosures
- CCTV
- Privacy notices, transparency and control
- ICO guidance - Anonymisation
- Personal Information Online Code of Practice

The Data Protection Act 2018

The Act regulates the processing of personal data about living identifiable individuals and provides individuals with rights in respect of data held about them. It applies to all personal data, not just to health and social care records. The same principles

therefore apply to records of employees held by employers, for example in finance, personnel and occupational health departments.

The General Data Protection Regulation



Individual rights under the GDPR

The GDPR confers rights on individuals that can be exercised in certain circumstances. In brief, an individual has

a) The right to be informed (articles 12 to 14)
b) The right of access (article 15)
c) The right to rectification (article 16 and 19)
d) The right to erasure (article 17 and 19)
e) The right to restrict processing (article 18 and 19)
f) The right to data portability (article 20)
g) The right to object (article 21)

h) The right not to be subject to automated decision making and profiling (article 22)

The right to be informed

This means that the Controller should provide information and communications relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, taking into account the age of the audience (e.g. Children). This is usually done through a Fair Processing Notification which will be on an organisations webpages, on posters or leaflets or using a mixture of all of these methods. There are certain criteria that need to be met and specific information included.

The General Data Protection Regulation (GDPR) makes transparency a priority. Information notices need to be clear and concise, and provide more extensive information than previously. Amongst other things, notices under GDPR must include new areas such as:

- Details of the Data Protection Officer.
- The legal basis for processing.
- Details of data transfers outside the EU.
- If possible, the retention period the data will be kept for.

There are also new rules on when the organisation must provide the information to the individual depending on whether the data is obtained directly from the individual or from another source.

Requests under the right of Access (Subject Access Requests)

Under the Data Protection legislation, all living individuals or 'Data Subjects' have a right to be informed of the following:

- If an organisation holds, stores or processes personal data about them
- A description of the categories of data held, the purposes for which it is processed and to whom it may be disclosed
- A copy of any information held
- To be informed as to the source of the data held
- Where automated decision-making has taken place, data subjects must be informed about the logic involved and envisaged consequences of such processing for the data subject

The right to rectification

An individual can exercise the right to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. You have one calendar month to respond to a request. In certain circumstances you can refuse a request for rectification.

The right to erasure

An individual has the right to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. You have one month to respond to a request. The right is not absolute and only applies in certain circumstances.

The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, you are permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing. You have one calendar month to respond to a request. This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view access and use their personal consumption and transaction data in a way that is portable and safe.

The right to object

Individuals can object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

You must stop processing the personal data unless: you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims. You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

The right not to be subject to automated decision making and profiling

The GDPR has provisions on: automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them. You can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent

You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:

- ✓ give individuals information about the processing;
- ✓ introduce simple ways for them to request human intervention or challenge a decision;
- ✓ carry out regular checks to make sure that your systems are working as intended

Relevance to the Caldicott Principles

The Data Protection legislation and Caldicott principles translate into **key rules for all staff to follow:**

- ✓ Patients and staff should be fully informed about how their information may be used
- ✓ There are strict conditions under which personal and Special categories of personal data may be disclosed
- ✓ Individuals have legislated rights including the right to information, the right of access, the right to rectification and erasure, the right to restrict processing, the right to data portability and the right to object to various types of processing of their data
- ✓ Identifiable information should be anonymised or pseudonymised wherever and whenever possible
- ✓ The disclosure or sharing of personal data is permissible where there is a legal obligation to do so, an exemption can be applied or where the individual has given explicit consent
- ✓ Sharing of personal data between organisations must take place with appropriate authority, safeguards and agreements in place
- ✓ Sometimes a judgement has to be made about the balance between the duty of confidence and disclosure in the public interest. Any such disclosure must be justified
- ✓ Personal data should be kept secure and confidential at all times

- ✓ An organisation must be able to provide evidence to show compliance with the data protection legislation requirements and principles

The lawful processing requirement

To be lawful the organisation must ensure all relevant rules of law (whether derived from legislation or common law) are complied with when processing personal data. This means that organisations must also comply with the common law duty of confidentiality.

Patients and service users provide care organisations with their information in the expectation that such information will be held confidentially and that it will not be disclosed to others without their consent.

Confidentiality

Everyone working in or for the NHS has the responsibility to use personal data in a secure and confidential way. Staff who have access to information about individuals (whether patients, staff or others) need to use it effectively, whilst maintaining appropriate levels of confidentiality.

The common law of duty of confidentiality requires that information that has been provided in confidence may be disclosed only for the purposes that the subject has been informed about and has consented to, unless there is a statutory or court order requirement to do otherwise.

Confidential Personal Information

Although an organisation within the NHS may have identified a lawful basis to process data, including special categories of personal data, this does not necessarily mean that the information can be used or shared in a way that identifies the individual if that information has been obtained where a 'duty of confidence' is owed.

In practical terms this means that if a GP wanted to share information with another care organisation that is providing care to that Patient e.g. an acute or community hospital, as long as the GP believes that the Patient would raise no objection and that it would be within their reasonable expectations for them to do this then this sharing is permitted and encouraged within the law. If however the GP wishes to share information that identifies a Patient and was obtained confidentially with someone else e.g. a charity, an advocate or a CCG, unless there are reasons why this must happen due to statutory obligations or it is in the public interest to do so, the Patient must be given the opportunity to consent to this happening.

What is Personal Data?

As described in part 1, subsection 3 of the Data Protection act 2018

(2) “Personal data” means any information relating to an identified or identifiable living individual
(3) “Identifiable living individual” means a living individual who can be identified, directly or indirectly, in particular by reference to —

(a) An identifier such as a name, an identification number, location data or an online identifier, or
(b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

Article 4 (1) of the GDPR, describes ‘personal data’ as any information relating to an identified or identifiable natural person (data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Therefore the terms living individual and natural person are interchangeable.

What are “Special Categories of Personal Data”?

As described in article 9 of the GDPR, special categories of personal data are Personal Data revealing:

a) racial or ethnic origin
b) political opinions
c) religious or philosophical beliefs
d) trade union membership
e) the processing of genetic data
f) biometric data for the purpose of uniquely identifying a natural person
g) data concerning health or
h) data concerning a natural person’s sex life or sexual orientation

Under the **Data Protection legislation** staff can only process or have access to personal data if:

- An appropriate condition for processing (GDPR Article 6 and Article 9) and a supporting lawful basis has been identified and where necessary, documented in a statutorily required (DPIA) or,
- Explicit consent has been obtained from the individual or,
- The data has been anonymised or pseudonymised in line with Data Protection legislation requirements; or
- The data is in respect of safety, safeguarding or in the public interest. Any decision taken to share Personal or Special Categories of Personal Data that is by its nature, owed a duty of confidentiality as a result of the above should be discussed with the DPO, documented in the DPIA and agreed by the Caldicott Guardian

The Conditions for processing under the GDPR (the Legal basis)

Article 6 conditions for processing personal data are as follows:
a) The Data Subject has given explicit consent
b) It Is necessary for the performance of a contract to which the data subject is party
c) It is necessary under a legal obligation to which the Controller is subject
d) It is necessary to protect the vital interests of the data subject or another natural person
e) It is necessary for the performance of a task carried out in the public interest or under official authority vested in the Controller
f) It is necessary for the legitimate interests of the Controller or third party (can only be used in extremely limited circumstances by Public Authorities and must not be used for the performance of the public tasks for which the authority is obligated to do)

Article 9 conditions for processing Special Categories of personal data are as follows:
a) The Data Subject has given explicit consent
b) For the purposes of employment, social security or social protection
c) It is necessary to protect the vital interests of the data subject or another natural person where they are physically or legally incapable of giving consent
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members
e) The data has been made public by the data subject
f) For legal claims or courts operating in their judicial category
g) Substantial public interest
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 (see note below)
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

Answer both questions, and then go to Knowledge check to check your answers.

Knowledge Check - Data Protection Legislation

Special Categories of Personal Data include? Tick **two or more options** from the answers listed below		
A	data concerning health	
B	religious or philosophical beliefs	
C	racial or ethnic origin	
D	A persons bank account number	

Knowledge Check - Data Protection Legislation - Fair processing

Under the Data Protection Legislation, who is responsible for providing fair processing information where a patient/services user is receiving health and social care services within a multi-agency setting? Tick **one option** from the answers listed below.		
A	Only the health organisation	
B	Neither the patient's GP should provide the information	
C	Both organisations, though one can inform people on behalf of the other	
D	Only the social care organisation	

Other relevant legislation

There is a range of legislation that impacts on the confidentiality agenda; the most relevant legislation includes the Acts below.

The Human Rights Act 1998

The Act incorporates the European Convention on Human Rights into UK law, allowing an individual to assert their Convention rights in UK courts and tribunals, rather than at the European Court in Strasbourg.

The Convention rights can be sought only against a public body, including NHS and local authorities. Article 8 of the Convention – the right to respect for private and family life – may be relevant to subject access requests, and to consent, confidentiality and disclosure issues.

The Freedom of Information Act 2000

The Act creates a general right of access to recorded information held by public authorities. Public authorities are required to make information available through a publication scheme and on request.

The NHS Act 2006

Section 251 of the National Health Service Act 2006 (and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002), enables the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be disclosed for medical purposes, where it is not possible to use anonymised information and where seeking consent is not practical, having regard to the cost and technology available.

In practice, this means that the person responsible for the information (the data controller) can, if they wish, disclose the information to the applicant without being in breach of the common law duty of confidentiality. The discloser must still comply with all other relevant legal obligations e.g. the Data Protection Legislation.

Medical purposes include medical research (that has received ethical approval by a research ethics committee) and the management of health and social care services. An application for Section 251 approval must be made to the Confidentiality Advisory Group of the Health Research Authority.

Knowledge Check - Data Protection Legislation - Lawful processing

The Data Protection Legislation requires personal data to be processed lawfully, what additional laws must be complied with? Tick **two or more options** from the answers listed below, and then go to Knowledge check to check your answer.		
A	The common law duty of confidentiality	
B	None, the Data Protection Legislation is sufficient	
C	The Human Rights Act	
D	The Freedom of NHS Act	

Summary

To make sure that patient or service user information is used properly, you will need to be familiar with the:

- Common law duty of confidentiality.
- Caldicott Principles.
- Confidentiality NHS Code of Practice.
- Relevant legislation and guidance, in particular the Data Protection Act 2018 and the GDPR.

Applying law and guidance

As you become more knowledgeable about the relevant areas of law, guidance and best practice, you will find that you are better able to apply your skills to different

scenarios and to better appreciate the considerations you must make to reach a reasoned decision.

The following eight scenarios illustrate examples of confidentiality and information sharing issues that typically would be within the remit of the Caldicott Guardian.
The examples cover issues such as access to clinical data, assisting a criminal investigation and deciding what can be revealed in the public interest.

Scenario 1: Internal information processing

Breaches of confidentiality can occur for quite mundane reasons and, as in this example, even with good intent but that doesn't prevent them being a serious issue that requires guidance.

You receive a letter from a service user complaining that her confidentiality has been breached. The service user has applied to become a governor of your organisation and has made a declaration regarding her eligibility to do so.

She believes that a member of Corporate Services has accessed her records to verify her declaration i.e. that she was a service user, and that they then proceeded to access the rest of the clinical record. At no time was her consent sought. Your investigations reveal that the content of the clinical record was accessed.
The staff member states that he accessed the record and the clinical content to confirm that the service user was eligible to represent users of cancer services. He further tells you that he cross-checks all applications to serve as governor in this way.

Why this was a breach of confidentiality

The action taken by the employee in accessing clinical data disregards the following provisions.

The Caldicott Principles	
Principle 1: Justify the purpose(s) for using confidential information	The employee had no valid reason for accessing the clinical record to check eligibility.
Principle 2: Only use confidential information when absolutely necessary	The eligibility checks could be carried out without use of clinical information.
Principle 3: Use the minimum that is required	There was no necessity to do more than check that the service user was on the patient administration system.
Principle 4: Access should be on a strict need-to-know basis	There was no need for non-clinical staff to access the clinical information to properly perform their role.
Principle 5: Everyone must understand his or her responsibilities	There was a clear indication that the staff member was either not aware of his

	responsibilities or had chosen to disregard them.
Principle 6: Understand and comply with the law	The key legal obligations breached are the common law duty of confidence and the Data Protection Legislation.
Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality	There was no duty to share the information in the care record and, in fact the duty to ensure it was not used for this purpose was greater.

Data Protection principles have been breached in this scenario:

Principle 1: Processed fairly, lawfully and in a transparent manner **Principle 2:** Collected for specified, explicit and legitimate purposes

Fair processing: the accessing of the clinical information should have been carried out in an open and transparent way, so that individuals are not misled as to who will have access to their data. This means that staff should have informed the service user that her data would be accessed before doing so.

Lawful processing: the processing must be carried out in accordance with all relevant laws. It is important to remember that information obtained for healthcare purposes is subject to the common law duty of confidentiality. This means that information given in confidence should not normally be further disclosed without the consent of the confider.

The staff member was wrong to have accessed the data in the way that they did, but what should have happened? The organisation does need to confirm the validity of the application and also needs to verify that the criteria are met regarding representation of a particular constituency.

However, the service user's consent should have been sought to ascertain whether she was on the patient administration system and no clinical information should have been accessed.

In future, a consent form seeking permission to check that an applicant is on the register of patients should be included with the governor application forms.

Scenario 2: Sharing information in the public interest

The anaesthetic department is reviewing the information they provide to patients discharged from the day surgery unit. Patients are advised before surgery that they should not drive for at least 48 hours after having a general anaesthetic. Occasionally, the patient is recovered and then wishes to drive themselves. Following a policy review it is decided that the pre-operative leaflet will be updated to

inform patients that the police will be notified if the patient states that they intend to drive themselves home whilst recovering from a general anaesthetic. Your advice is sought on whether such a disclosure would fall into the category of 'in the public interest'.

The common law duty of confidentiality

One of the considerations to be made in this case is whether disclosing this information to the police would breach the common law duty of confidentiality.

The Confidentiality NHS Code of Practice and the General Medical Council guidance: 'Confidentiality' set out the circumstances under which a disclosure of confidential information without consent is permitted if it is in the substantial public interest to disclose. The common law of confidentiality is applicable to both living and deceased individuals.

Deciding whether it is in the substantial public interest to disclose

The discloser must decide whether the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service. One example of where disclosure of personal information without consent may be justified in the public interest is where failure to disclose may expose the patient or others to risk of death or serious harm.

Risk of death or serious crime to others

Clinicians also have a duty of care to people other than the patient, i.e. there are times when the health and safety of others must take precedence. If the discloser is of the view that disclosure is necessary to protect a third party from death or serious harm, the information should be promptly reported to an appropriate person or authority.

Effect of general anaesthetic

A second consideration is the length of time that impairment of driving ability is likely to last in a person recovering from day case surgery under general anaesthetic. According to the Royal College of Anaesthetists impairment will vary (generally lasting between 24 to 48 hours) depending on the type of surgery; the length of time the patient is anaesthetised; and other patient-specific factors.

However, it is accepted practice that patients must be informed that they should not drive on the same day that they have received a general anaesthetic. This can be emphasised by informing them that their insurance is likely to be invalid if they do so.

Clear evidence of danger

If a situation arises where a specific patient insists on driving despite there being **clear evidence** that he/she is likely to be a danger and to pose a significant "risk of death or harm" to themselves or to others, then there may be a public interest duty of disclosure which overrides the duty of confidentiality.

The disclosure, if made, should be in line with the Confidentiality NHS Code and the GMC's guidance both of which are available via the **Resources** section of this workbook.

Additionally, patient communication materials should be updated, and staff should check that the patients are aware of and have understood the information before they have their surgery. Possible wording for the communication materials could be:

"We will inform the police if we believe you are still significantly affected by general anaesthetic and you ignore our advice not to drive."

Knowledge Check: Public interest

What information might you be justified in disclosing about a patient/services user to protect a third party from serious harm? Tick **one option** from the answers listed below, and then go to Knowledge check to check your answer.		
A	The entire clinical /care record	
B	None, you are prevented by the Data Protection Legislation	
C	The minimum necessary for the purpose	
D	None, you are prevented by the common law duty of confidentiality	

Scenario 3: Disclosure to assist a criminal investigation

You are the Caldicott Guardian at a local care organisation and have been asked for your advice on a disclosure of information to the police regarding a fly-tipping case. On Monday rubbish was seen being dumped near your organisation from a van. A witness saw a similar van go into the organisation's car park soon afterwards where a man got out and went into the building. The police have requested access to that month's car park CCTV recordings to investigate the matter.

What advice would you give? Read each option carefully then pause to consider which answer you would give. When you have finished, read the feedback to see if you were correct.	
A	We must grant the request as the Data Protection Legislation requires that we give the police all of the CCTV recordings that were made that month.
B	We could grant the request as the Data Protection Legislation permits us to give the police all of the CCTV recordings made that month.
C	We could meet some of the request as the Data Protection Legislation permits us to give the police the CCTV recording for the specific date that the alleged offence occurred.

D	We cannot grant any of the request as the Data Protection Legislation prevents us from giving the police any of the CCTV recordings that were made that month.

Feedback

The Data Protection Legislation *permits* the disclosure of personal information without consent subject to specific constraints.

Data Protection Act 2018, Schedule 1, part 2 - Substantial public interest conditions, paragraph 10 states that

Preventing or detecting unlawful acts

(1) This condition is met if the processing—
(a) is necessary for the purposes of the prevention or detection of an unlawful act,
(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and
(c) is necessary for reasons of substantial public interest.

(2) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

(3) In this paragraph—
"Act" includes a failure to act;
"Competent authority" has the same meaning as in Part 3 of this Act (see section 30) which is derived from Schedule 7 and applies to Chief Officers of police and other policing bodies and those acting under their authority.

The decision to disclose must be made on a case-by-case basis with disclosure only if there is a strong public interest justification for doing so. Where disclosure is justified it should be limited to the **minimum necessary** to meet the need and the service user should be informed of the disclosure unless it would defeat the purpose of the investigation, allow a potential criminal to escape or put staff or others at risk.

In the scenario above there should be notices for Patients informing them that their use of the car park is covered by CCTV and therefore this may be requested by the Police if required.

Knowledge Check: Disclosure to the police

What would you consider if you were consulted about disclosing personal

information about a patient/service user to the police? Tick **two or more options** from the answers listed below, and then go to Knowledge Check to check your answer.		
A	Whether the individual should be informed of the disclosure	
B	Whether there is strong public interest justification for the disclosure	
C	Whether the law permits you to share the information	
D	Whether the police are insistent in their request	

Scenario 4: In a different light

A member of staff informs you that the police have requested information from your organisation and have told him that the law requires the organisation to provide the information. What advice do you provide?

Disclosures required by legislation

Some statutes place a strict requirement on organisations to disclose information. You should make sure the police have provided the name of the statute and the relevant section requiring disclosure so that you can be certain the organisation is required to disclose. If necessary, you should ensure your organisation's legal advisors provide an opinion. If the relevant statute has been properly cited, you should take care to only disclose the information required to comply with and fulfil the purpose of the law.

If you have reason to believe that complying with a statutory obligation to disclose information would cause serious harm to the patient/service user or another person, you should seek legal advice.

Legislation requiring disclosure

Examples of legislation requiring disclosure include:

- Public Health (Control of Disease) Act 1984 - requires notification to the Health Protection Agency of specified diseases and food poisoning incidents.
- Road Traffic Act 1988 - requires health professionals to provide to the police information which might identify a driver alleged to have committed a traffic offence.
- NHS Act 2006 - gives powers to investigators of fraud in the NHS to access confidential patient information.
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1985 - requires employers to report deaths, certain diseases, dangerous occurrences, major injuries, and accidents resulting in more than three days off work.
- Terrorism Act 2000 - requires all citizens to inform police as soon as possible of any information that may help to prevent an act of terrorism, or help in apprehending or prosecuting a terrorist.

- Medical Act 1983 - gives the General Medical Council powers to request access to a patient's records to investigate a doctor's fitness to practice. Unless you are the doctor under investigation, you are obliged to comply with that request.
- The Child Support (Information, Evidence and Disclosure) Regulations 1992 – require certain categories of people (including local authorities) to provide such information or evidence as is required by the Secretary of State to enable him to make certain decisions under the Child Support Act 1991 (regulation 2).

Disclosures required by court order

The courts, including coroner's courts, and some tribunals and persons appointed to hold inquiries have legal powers to require that information that may be relevant to matters within their jurisdiction be disclosed. This does not require the consent of the patient/service user whose records are to be disclosed but they should be informed, preferably prior to disclosure.

Disclosures must be strictly in accordance with the terms of a court order and to the bodies specified in the order. If you are concerned that a court order requires disclosure of sensitive information that is not relevant to the case in question, you may raise ethical concerns with the judge or presiding officer. If however, the order is not amended it must be complied with.

Knowledge Check: Disclosures required by law

What are the circumstances under which your organisation could be compelled to disclose personal information? Tick **two or more options** from the answers listed below, and then go to Knowledge check to check your answer.		
A	To comply with a court order	
B	To comply with legislation	
C	There are no such circumstances	
D	To comply with the Chief Executive's request	

Scenario 5: Subject access request under the Right of Access

You are the Caldicott Guardian for Adult Social Services at a local authority and you have been asked for your advice regarding a subject access request. A service user has asked for a copy of the whole of his social care record. The member of staff managing the request has discovered that the record also contains health information supplied by the local NHS Trust.

The member of staff wants to know whether the complete record should be disclosed or if the health information should be kept back? Below are three questions you need to consider.

1. Does the fact that NHS information has been shared with and incorporated into social services documentation, mean that it ceases to be 'NHS information'?
2. Are social services entitled to keep back the health information, or are they obliged to disclose everything they have recorded?
3. Do social services even need to disclose that they are holding health information?

Disclosing information

Confidential information should only be disclosed outside of the organisation that it was given to (whether health or care) if the discloser is satisfied that the recipient organisation has policies and procedures in place to hold the information confidentially and securely.

Importantly, the service user should have been informed by the NHS Trust prior to the disclosure that confidential information was to be transferred to social services. The disclosure does not transform the information; it remains the information of the disclosing organisation. This means that the disclosing organisation continues to have liabilities in respect of the information.

The recipient organisation cannot further disclose the information without consent or other legal basis, i.e. they are not entitled to share the information just because they have it in their possession. The recipient organisation may wish to inform the applicant that further information is available from another organisation - in this case the NHS Trust.

Scenario 6: Access to records of the deceased

A Freedom of Information request is received for the care records of a number of service users who died whilst receiving community care services from your organisation. Would you be justified in meeting the request?

Read each option carefully then pause to consider which answer you would give; then read the feedback to see if you were correct.		
A	No, the Data Protection Legislation prevents us from releasing the information	
B	Yes, the Access to Health Records Act 1990 permits us to release the information	
C	Yes, the Freedom of Information Act 2000 requires us to release the information	
D	No, the common law duty of confidentiality prevents us from releasing the information	

Feedback

No, the Data Protection Legislation prevents us from releasing the information

This is incorrect.

The Data Protection Legislation applies only to the personal data of living individuals and there is no provision within it to withhold the data of the deceased.

Yes, the Access to Health Records Act 1990 permits you to release the information

This is incorrect.

The Access to Health Records Act does not apply to social care records.

In terms of health records it does apply to the records of deceased patients, however it only provides access rights to personal representatives (the person or people who administer the deceased's estate under the law relating to wills and probate) of the deceased and persons having a claim arising from the death of the patient.

Yes, the Freedom of Information Act 2000 requires us to release the information:

This is incorrect.

Section 41 of the Act states that information will be exempt from disclosure if it was obtained from a person or organisation other than the person making the FOI request and disclosure would result in a breach of confidence over which a person could take legal action (i.e. it would be an actionable breach of confidence).

To determine whether there would be an actionable breach of confidence if the information was disclosed, you need to consider the following:

- *Whether the information is in fact confidential*: a duty of confidence arises when one person discloses information to another (e.g. service user to social worker; patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It is probable that much of the information contained in the care record would have been originally obtained from the deceased meaning that it has the necessary quality of being confidential information.
- *Whether there is someone with the legal standing to take action*: the duty would be legally enforceable by the deceased's personal representative - the person or people who administer the deceased's estate under the law relating to wills and probate.

The Information Tribunal (in the case of Mrs. P Bluck v The Information Commissioner and Epsom and St Helier NHS Hospital Trust, 17th Sept 2007, EA/2006/0090, see: http://www.informationtribunal.gov.uk/Documents/decisions/mrspbluckvinformationcommissioner17sept07.pdf) stated that the duty of confidentiality does continue after the death of an individual to whom that duty is owed. Where there is a legally enforceable duty of confidentiality owed to a living individual, after death it can be enforced by the deceased's personal representative.

No, the common law duty of confidentiality prevents you from releasing the information

This is correct.

It has been confirmed by the Information Tribunal (in the case of Mrs. P Bluck discussed above) that the duty of confidentiality does continue after the death of an individual to whom that duty is owed. Where there is a legally enforceable duty of confidentiality owed to a living individual, after death it can be enforced by the deceased's personal representative. It is not necessary to establish that, as a matter of fact, the deceased person actually has a personal representative who would take action. This principle is of particular relevance to those public authorities holding records on an individual's personal details, such as health records or the provision of social care. The Information Commissioner followed the decision in Bluck in a Decision Notice directed at NHS North Tyneside Clinical Commissioning Group in May 2015 see: https://ico.org.uk/media/action-weve-taken/decision-notices/2015/1431776/fs_50568280.pdf

Knowledge Check - Access to deceased patients' records

Which categories of people have a legal right of access to deceased patient records? Tick **two or more options** from the answers listed below, and then go to page 58 to check your answer.

A	Persons with a claim arising from the death	
B	The patient's next of kin	
C	Executors of the deceased patient's will	
D	All clinicians	

Scenario 7: Sharing non-confidential personal information without consent

Your advice is sought on whether for integrated care purposes, names and addresses can be shared by your Local Authority with NHS Digital or a health body to trace NHS Numbers for the named individuals. What should you consider?

Is the information sensitive or confidential?

Personal information is categorised by the Data Protection Legislation under distinct categories see what is Personal Data? And what are "Special Categories of Personal Data"?

Basic contact details - name and address and NHS Number etc. - which do not reveal anything confidential about an individual and are essentially already in the public domain, may be shared between organisations providing the provisions of the Data Protection Legislation can be satisfied. These provisions require that the purpose of sharing is related to the activities that your organisation is there to deliver and that reasonable steps to inform the individuals concerned about the sharing have been taken. Note that whilst consent is not required, in most circumstances any objections raised by individuals should be respected.

What is the purpose of the sharing?

One of the most common reasons for wishing to share non-confidential information is to identify a cohort of individuals who have particular characteristics. As Caldicott Guardian you need to be aware of these types of sharing requests, because the act of sharing makes these characteristics known to the recipient and this can result in confidential information being learned inappropriately.

Where the information concerned is defined as a 'Special Category of Personal Data' by the Data Protection Legislation, additional care is required because consent is only one of the possible options for meeting the requirements.

Data Protection Impact Assessments (DPIAs) are a useful tool for developing an understanding of the consequences of sharing and therefore whether there is a need for a more specific legal basis to support the proposed sharing. Inevitably an element of judgement is required but engaging with local patient/service user groups and other professionals to determine their views as part of the DPIA process, and ensuring that controls limit access to those who need to know the information to do their work can help with this.

Examples

The following examples will hopefully assist with the required assessment and judgement.

Identifying which individuals in a care home have attended A&E: A Local Authority could share a list of individuals in a care home with an NHS Trust without breaching confidentiality or revealing sensitive data. However, the reverse is not the case as the fact of an A&E attendance is itself confidential.

Options: The NHS Trust could provide aggregated 'hot spot' data showing numbers of care home residents that have attended A&E by care home over a specified period. Where an individual has attended A&E on numerous occasions and the Trust has safeguarding concerns they could share these concerns about the identified individual in the public interest.

Identifying individuals with long term conditions who would benefit from social care interventions: The only basis for the NHS to share this confidential information is with the consent of the individuals concerned.

Identifying individuals in receipt of social care who are also receiving mental health care: A Local Authority could share a list of individuals with a Mental Health Trust without breaching confidentiality or revealing sensitive data. However, the Trust could not disclose details of which individuals were receiving mental health care without either consent, a public interest justification (e.g. risk to others) or, if an

individual lacks capacity the Trust could make a disclosure in the individual's best interests.

Scenario 8: Access to confidential patient information for clinical audit

A Clinical Commissioning Group (CCG) has requested access to confidential patient information held by your Trust for clinical audit purposes. Should you permit this sharing?

Providers owe a duty of confidentiality to their patients, and CCGs have no statutory power that enables them to override this duty. Therefore, to access identifiable and confidential patient information for clinical audit purposes a CCG will need a clear basis in law.

Legal basis

The legal basis must be one of:

- Explicit patient consent
- Section 251 approval following an application to the Confidentiality Advisory Group (discussed on page 31). Patients should be informed about the possibility of CCG access and be given the opportunity to object.
- Public interest

Public interest

Exceptionally, where there has been a serious incident or there are serious concerns about the care provided, you may agree that the public interest served by allowing a CCG to conduct a clinical audit of identifiable patient records is sufficient to warrant overriding the duty of confidentiality.

Options

If it is practicable for your organisation to generate an anonymised view of a record, so that the CCG does not have the capacity to identify the patients concerned, this would be lawful.

Summary

The cases discussed illustrate some of the knowledge you will need to apply to make a decision.

In many cases, there is no clear 'right or wrong' answer but you should do your best to ensure the decision you arrive at is a reasonable one in all the circumstances of the case. Considerations such as these illustrate why Caldicott issues often require a decision to be made on a case-by-case basis. Although the differences in cases

might seem to be minor they can easily lead to a different, and equally valid, decision being made.

Resources for Caldicott Guardians

The UK Caldicott Guardian Council

There are several avenues of support and guidance that will help you in carrying out your role as Caldicott Guardian. Your first port of call should be the UK Caldicott Guardian Council. The Council is an elected body made up of Caldicott Guardians from health and social care.

Their website is at: Caldicott Guardian Council.

As part of their role, the Council provides advice on the resolution of Caldicott queries. If you would like to find out more about the Council or seek their advice, you can contact the Secretariat at ukcgcsecretariat@nhs.net.

Your professional body or medical defence union may also provide advice on confidentiality issues.

The Information Governance Alliance

The Information Governance Alliance (IGA) is the authoritative source of advice and guidance about the rules on using and sharing information in health and care. The core members of the IGA are the Department of Health, NHS England, NHS Digital and Public Health England. Representatives from the Information Commissioner's Office and the National Data Guardian's Office also sit on the Board.

The IGA offers advice and support, develops networks, publishes guidance, endorses guidance produced by others, and works with local and national organisations to improve knowledge and practice of information governance across the health and care system. You can access guidance, the IGA newsletter, and information about events from their website at: The Information Governance Alliance

The IGA can be contacted via exeter.helpdesk@nhs.net.

NHS Digital - External Information Governance

The External Information Governance Delivery team at NHS Digital works closely with the IGA, and provides advice and guidance for IG queries via the IG helpdesk at: exeter.helpdesk@nhs.net.

Guidance and websites

Guidance

- A Manual for Caldicott Guardians. London: UKCGC, 2017
- Confidentiality: NHS Code of Practice. London: DH, 2003.
- Confidentiality: NHS Code of Practice Supplementary Guidance - Public Interest Disclosures London: DH, 2010.
- Resources for Information Sharing. Leeds: IGA, 2017
- Caldicott 1 - Report on the Review of Patient-Identifiable Information. London: Caldicott Committee, 1997
- Caldicott 2 - Information: To Share Or Not To Share? The Information Governance Review. London: Independent Information Governance Oversight Panel, 2013
- Caldicott 3 - Review of Data Security, Consent and Opt-Outs. London: National Data Guardian, 2016
- Confidentiality 2017. London: General Medical Council, 2017
- Confidentiality and Health Records Toolkit. London: British Medical Association

Acts of Parliament

- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000

Websites

- UK Caldicott Guardian Council
- Information Governance Alliance
- National Data Guardian

Cases

- Mrs P Bluck v The Information Commissioner and Epsom and St Helier NHS Hospital Trust, 17th Sept 2007, EA/2006/0090
- Information Commissioner Decision Notice - NHS North Tyneside Clinical Commissioning Group in May 2015

Answers to Knowledge check questions

Knowledge Check - Qualities of a Guardian: Which of the following knowledge and experiences are you likely to need to carry out the role?		
A	Extensive knowledge of legal issues	
B	Knowledge of how information is used and shared	**X**
C	Experience of drafting Information Governance policies	
D	Experience of working at a senior level	**X**

Knowledge Check - Who should be the Caldicott Guardian?: Based on the scenario, would Jennifer be justified in recommending that she takes on the role of Caldicott Guardian herself?		
A.	Yes	
B.	No	**X**

Feedback: Although Jennifer has some experience as an IG manager and, before that, as a social worker, and is doubtless very knowledgeable about key guidance and legislation, she does not have the required level of seniority to champion Caldicott issues at Senior Management Team level and be the final arbiter on complex confidentiality issues.

Knowledge Check - Working with the SIRO: The role of SIRO is distinct from the role of the Caldicott Guardian, which of the following are part of the SIRO role?		
A	Providing organisational direction for data handling and information risk management	**X**
B	A point of contact for information incidents	**X**
C	Providing an advisory service to the organisation	
D	Ensuring that patient/service user information is used to provide effective care	

Knowledge Check - Working with the DPO: The role of DPO is distinct from the role of the Caldicott Guardian, which of the following are part of the DPO role?		
A	Ensuring the organisation undertakes all of the necessary compliance and assurance checks required for the IG toolkit	**X**
B	A point of contact for information incidents with the Information Commissioners Office	**X**
C	Providing an advisory service to the organisation	**X**
D	Ensuring that patient/service user information is used according to Data Protection Legislation	**X**

Knowledge Check - Information Governance: How does your role support the wider information governance agenda?		
A	Ensuring the Board is fully informed of any confidentiality concerns	**X**
B	Ensuring the arrangements for confidentiality and data protection are monitored by the DPO	**X**
C	Carrying out internal audits relating to confidentiality and data protection assurance	
D	Arranging external auditors to carry out confidentiality and data protection assurance audits	

Knowledge Check - Responsibilities of the role: How can the Caldicott Guardian help to ensure that confidentiality is embedded into the organisation? Tick **two or more options** from the answers listed below.		
A	Ensuring the Board / senior management team are adequately informed about confidentiality issues	**X**
B	Ensuring that confidential information is not shared for clinical/care purposes	
C	Ensuring staff are provided with clear guidelines and procedures	**X**
D	Ensuring that identified improvements to confidentiality processes are implemented	**X**

Knowledge Check - Sharing demographic information: If you supply the information as requested, have you breached the Caldicott Principles?		
A.	No. It's an important request from the police and the information should be supplied	
B.	No. The police are not asking for clinical/care information so this information can be supplied	
C.	Yes. The police are not asking for clinical/care information but even so the information should not be supplied	**X**
D.	Yes. But it's an important request from the police and if it helps to locate the person it is in the public interest	

Feedback: You should **not** supply the information, even though it is not clinical/care information; the rules of the common law duty of confidentiality still apply. Your organisation only holds information about 'John Smith' because he is a service user and has provided this information in confidence in order to receive those services. Generally such information should not be further disclosed without the consent of the provider. In the scenario given there is no justified reason for sharing this information with the police (Caldicott Principle 1) - adults have the right to be 'missing' if they so wish. If you want to assist the police, you could ask them to provide a letter that the organisation can forward to relevant service users.

Knowledge Check - Data Protection Legislation: Special Categories of Personal Data

include. Tick 2 or more options from the answers listed below.		
A	data concerning health	**X**
B	religious or philosophical beliefs	**X**
C	racial or ethnic origin	**X**
D	A persons bank account number	

Knowledge Check - Data Protection Legislation - Fair processing: Under the Data Protection Act, who is responsible for providing fair processing information where a patient/services user is receiving health and social care services within a multi-agency setting? Tick **one option** from the answers listed below.		
A	Only the health organisation	
B	Neither the patient's GP should provide the information	
C	Both organisation's, though one can inform people on behalf of the other	**X**
D	Only the social care organisation	

Knowledge Check - Data Protection Legislation - Lawful processing: The Data Protection Act requires personal data to be processed lawfully, what additional laws must be complied with? Tick **two or more options** from the answers listed below.		
A	The common law duty of confidentiality	**X**
B	None, the Data Protection Legislation is sufficient	
C	The Human Rights Act	**X**
D	The Freedom of NHS Act	

Knowledge Check - Public interest: What information might you be justified in disclosing about a patient/services user to protect a third party from serious harm? Tick **one option** from the answers listed below.		
A	The entire clinical /care record	
B	None, you are prevented by the Data Protection Legislation	
C	The minimum necessary for the purpose	**X**
D	None, you are prevented by the common law duty of confidence	

Feedback: The discloser must decide whether the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service.

One example of where disclosure of personal information without consent may be justified in the public interest is where failure to disclose may expose the patient or others to risk of death or serious harm.

The decision must be made on a case-by-case basis, and if it is decided to disclose, only the minimum information necessary for the purpose should be disclosed.

Knowledge Check - Disclosure to the police: What would you consider if you were consulted about disclosing personal information about a patient/service user to the police? Tick **two or more options** from the answers listed below.		
A	Whether the individual should be informed of the disclosure	**X**
B	Whether there is strong public interest justification for the disclosure	**X**
C	Whether the law permits you to share the information	**X**
D	Whether the police are insistent in their request	

Knowledge Check - Disclosures required by law: What are the circumstances under which your organisation could be compelled to disclose personal information? Tick **two or more options** from the answers listed below.		
A	To comply with a court order	**X**
B	To comply with legislation	**X**
C	There are no such circumstances	
D	To comply with the Chief Executive's request	

Knowledge Check - Access to deceased patients' records: Which categories of people have a legal right of access to deceased patient records? Tick **two or more options** from the answers listed below		
A	Persons with a claim arising from the death	**X**
B	The patient's next of kin	
C	Executors of the deceased patient's will	**X**
D	All clinicians	

Assessment

Attempt **all** of the following **20** questions; the pass mark is 80%. If you don't reach 80%, revise the relevant topics and try again.

Check with your IG lead whether your responses need to be recorded and logged.

Question 1: What qualities should a Caldicott Guardian have? Tick **two or more options** from the answers listed below.		
A	Sufficient experience and seniority to advise the Board on confidentiality issues	
B	Awareness of the key guidance on confidentiality	
C	Expertise in the field of Information Technology	
D	Extensive knowledge of all aspects of Information Governance	

Question 2: Which of the following options form part of the Caldicott Guardian's role? Tick **two or more options** from the answers listed below.		
A	To prevent all information sharing outside the organisation	
B	To make sure all patient and service user information is published	
C	To enable appropriate sharing of patient and service user information	
D	To protect the confidentiality of patient and service user information	

Question 3: Which of the following form part of the Caldicott Guardian's role? Tick **two or more options** from the answers listed below.		
A	To develop and influence confidentiality policy within the organisation	
B	To oversee information security management within the organisation	
C	To make instant decisions about uses of information	
D	To make practical decisions about uses of confidential information	

Question 4: The role of Caldicott Guardian is distinct from the role of the SIRO, which of the following are part of the Caldicott Guardian role? Tick **two or more options** from the answers listed below.		
A	Being legally accountable for all confidentiality issues	
B	Acting as the conscience of the organisation	
C	A point of contact for confidentiality issues	
D	Management of all patient information assets	

Question 5: What role does the Caldicott Guardian play if there is a breach of confidentiality? Tick **two or more options** from the answers listed below.		
A	Ensure the incident is not reported	
B	Review confidentiality procedures	
C	Take part in the lessons learned process	
D	Ensure that any misconduct results in disciplinary action	

Question 6: What role does the Caldicott Guardian play if there is a request to share confidential information? Tick **two or more options** from the answers listed below.		
A	Determine whether it is appropriate to share the information	
B	Advise the organisation on confidentiality measures	
C	Always say no!	
D	Permit sharing if it is to a colleague	

Question 7: What is the role of the Caldicott Guardian in relation to the wider information governance agenda? Tick **two or more options** from the answers listed below.		
A	Contribute to the reports provided for the Board / senior management team of confidentiality and data protection issues	
B	Advising the Board / senior management team with options for confidentiality and data protection improvement	

C	Contributing to the organisation's assurance statement	
D	Making sure confidentiality and data protection issues are not discussed at meetings of the Board / senior management team.	

Question 8: How can the Caldicott Guardian promote a confidentiality culture? Tick **two or more options** from the answers listed below.		
A	Rejecting all requests for sharing clinical/care information	
B	Ensuring staff have access to confidentiality training	
C	Drafting the organisation's risk management policy	
D	Raising confidentially resource concerns with the Board / senior management team	

Question 9: When resolving local confidentiality issues what information should be retained in a log to assist with future similar queries? Tick **two or more options** from the answers listed below.		
A	personal information about a patient/service user	
B	The time spent on resolving the issue	
C	The decision taken and reason for doing so	
D	The resources required to resolve the issue	

Question 10: You are asked for your advice on an information sharing issue, what should you consider? Tick **two or more options** from the answers listed below.		
A	Whether the patient has consented to the sharing	
B	Whether there is a genuine need to share the information	
C	Whether the request is from an important person	
D	Whether the other organisation shares information with you	

Question 11: Which of these are Principles under the GDPR?

A	The requirement to prevent the sharing of confidential information	
B	The requirement to collect personal data fairly	
C	The requirement to process personal data lawfully	
D	The requirement to process data securely	

Question 12: Under Data Protection Legislation individuals must be provided with fair processing information, which of the following statements is **incorrect**? Tick **one option** from the answers listed below.		
A	The fair processing information should be given to the individual at the earliest opportunity	
B	The fair processing information is required only for sensitive personal data	
C	The fair processing information should contain information about the purpose of the processing and who data is likely to be disclosed to	
D	The fair processing information should contain information about who the data controller is and the type of data being processed	

Question 13: Does the Data Protection Legislation require that consent is obtained before processing non-confidential personal information? Tick **one option** from the answers listed below.		
A	No, consent is just one of the conditions required for processing	
B	No, consent isn't relevant to the Data Protection Legislation	
C	Yes, without consent no personal information can be processed	
D	Yes, because personal data has to be processed in accordance with the rights of the individual	

Question 14: Would it be justified to use care records to target services users so you can send them details of a charity event? Tick **one option** from the answers listed below.

A	Yes, if the charitable aims are relevant to their condition	
B	No, because this is not an appropriate use of staff time	
C	No, as this is not the purpose the information was collected for	
D	Yes, as long as it is a charity related to the provision of health or care	

Question 15: What is the test for determining whether a disclosure of information is in the substantial public interest? Tick **one option** from the answers listed below.		
A	Whether the disclosure is interesting to the public	
B	Whether the public good would outweigh the obligation of confidentiality to the patient/service user	
C	Whether the public good would outweigh the obligation of confidentiality to the patient/service user and the broader public interest in providing a confidential service	
D	Whether the public good would outweigh the public interest in providing a confidential service	

Question 16: In what type of situations might it be reasonable to say it is sufficiently in the public interest to disclose personal information? Tick **two or more options** from the answers listed below.		
A	To protect the patient/service user from death or serious harm	
B	To assist the police to investigate a murder	
C	To assist the police to locate a missing adult when there is no evidence of there being a case of serious crime	
D	To protect the reputation of the organisation	

Question 17: A patient/service user has a history of violence; can this information be shared with other members of staff? Tick **one option** from the answers listed below.		
A	No, this is confidential information and cannot be shared	
B	Yes, with everyone in the organisation to protect them from serious	

	harm	
C	No, it can only be shared if the patient is violent again	
D	Yes, with staff in direct contact with the patient/service user	

Question 18: You are asked whether police can be informed of the name of a patient being treated for a non-accidental but minor knife wound, what would your advice be? Tick **one option** from the answers listed below.		
A	Disclose information about the fact of the incident only	
B	Disclose information about the fact of the incident and the patient identity	
C	Disclose information about the fact of the incident and if the police request further details, ask for patient consent regarding disclosing their identity	
D	Do not disclose anything at all	

Question 19: You are informed that you must disclose personal information to comply with legislation, what would you do? Tick **one option** from the answers listed below.		
A	Ask the requestor to come back with a court order	
B	Ask the requestor to provide details of the relevant legislation and seek legal advice if necessary	
C	Inform the requestor that the Data Protection Legislation prevents you from providing the requested information	
D	Inform the requestor that it would not be in the public interest to provide the requested information	

Question 20: What Act provides a right of access to deceased patient records for personal representatives? Tick **one option** from the answers listed below.		
A	The Freedom of Information Act	
B	The Data Protection Act 2018	

C	The Human Rights Act	
D	The Access to Health Records Act	

You have reached the end of this workbook.