hscic Health & Social Care Information Centre

Code of practice on confidential information

Code of practice on confidential information

Good practice guidance for organisations collecting, analysing, publishing or otherwise disseminating confidential information concerning, or connected with, the provision of health services or adult social care in England.

Published by the Health and Social Care Information Centre

Version 1.0
December 2014

www.hscic.gov.uk

The HSCIC is committed to building on this code of practice and updating it regularly, working with partners such as the Information Governance Alliance, and drawing on the experience of other organisations and sharing their practical examples of practice.
To provide feedback on this code of practice:

Tel: 0845 371 3671
Email: exeter.helpdesk@hscic.gov.uk

Contents

Foreword

Organisations that handle confidential health and social care information have to ensure that it is held securely and shared appropriately.

In publishing this document we are discharging our statutory duty to publish a code of practice on confidential information. This is the first step on a journey to provide recommended practice for organisations that collect, analyse, publish or disseminate confidential information.

We published the Guide to Confidentiality in Health and Social Care in September 2013 to provide advice to frontline staff and the public on the use of confidential information. This code of practice complements the guide by providing good practice guidance to individuals accountable for setting and implementing policy for organisations that are handling confidential information for purposes beyond direct care.

The code builds on Dame Fiona Caldicott's Information Governance Review: *To Share Or Not To Share?* by describing necessary and good practice, and providing practical examples.

We are committed to building on this code and updating it regularly, working with partners such as the Information Governance Alliance, and drawing on the experience of other organisations and sharing their practical examples of practice.

Andy Williams
Chief Executive
Health and Social Care Information Centre

Introduction

About this guidance

People should feel confident that health and social care bodies handle confidential information[1] appropriately.

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.

Caldicott principle 7.

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

This code of practice describes good practice for organisations handling confidential information concerning, or connected with, the provision of health services or adult social care. It therefore has a particular scope. Various information regimes will apply to these practices, including; the Data Protection Act, the Freedom of Information Act, Environmental Regulations and general data security and information governance guidance. For further information in relation to these areas please visit:

- Data protection act
  http://ico.org.uk/for_organisations/data_protection.
- Freedom of information act
  http://ico.org.uk/for_organisations/freedom_of_information.
- Environmental regulations
  http://ico.org.uk/for_organisations/environmental_information.
- Information Governance Toolkit
  www.igt.hscic.gov.uk

This code of practice is provided in response to the Health and Social Care Act 2012, section 263 that requires:

- The Health and Social Care Information Centre to publish a code of practice on the actions to be taken in relation to the collection, analysis, publication or other dissemination of confidential information concerning or connected with the provision of health services or of adult social care in England,
- The approval of the Secretary of State and the Board[2] (so far as the code relates to information concerning or connected with, the provision of NHS services) to its publication, and

1 This code of practice uses a specific definition of confidential information defined in the Health and Social Care Act 2012, section 263

2 The Board refers to the NHS Commissioning Board, known as NHS England

- That health and social care bodies carrying out functions related to the provision of health services or adult social care in England and persons, other than public bodies, who provide health services or adult social care in England pursuant to arrangements made with a public body exercising functions in connection with the provision of such services or care to have regard to this code of practice.

In preparing this code the Health and Social Care Information Centre has sought to minimise the burdens it imposes on others.

Who must have regard to this code of practice?

The primary audience for this code of practice therefore comprises individuals accountable for setting and implementing organisational policy, within the organisations set out in the 'Scope' section below.

Scope

What is in scope?

The code of practice has been prepared by the Health and Social Care Information Centre for:

- health or social care bodies that collect, analyse, publish or otherwise disseminate confidential information concerning, or connected with, the provision of health services or of adult social care in England[a], and
- persons other than public bodies who provide health services or adult social care in England pursuant to arrangements made with a public body[b] exercising functions in connection with the provision of such services or care.

Where an organisation meets these criteria then it **must** have regard to this code of practice.

Although record keeping by a health or care provider for an individual is not in scope, subsequent collection, analysis, publication or dissemination of confidential information based on a care record is within the scope of this code of practice.

Individuals and organisations **may** receive confidential information through a data sharing agreement requiring them to have regard to this code of practice. In such a case they **must** have regard to this code of practice.

Informative flow charts have been included in Annex 1 on page 25 to assist in determining the scope of this code of practice.

What is not in scope?

The code of practice does not apply to the direct provision of care, related record keeping or documentation facilitating the handover of care from one care provider to another. In September 2013 we published A guide to confidentiality in health and social care[3] as guidance to support direct provision of care.

It does not as such extend to the Health and Social Care Information Centre's system delivery functions,[c] that is the functions of development or operation of information or communications systems in connection with the provision of health services or of adult social care, except for any component of those systems that consists of the collection, analysis, publication or other dissemination of confidential information in connection with the provision of such services. Examples of systems delivery functions include the Spine

3 www.hscic.gov.uk/confguide

services, Summary Care Record and the Electronic Prescription Service, but any of these may include components that involve the collection, analysis, and publication or other dissemination of confidential information to which activities the code may apply.

In line with the Health and Social Care Act 2012, this code of practice does not apply to confidential information solely concerning or connected with:

- children's social care or
- services provided outside England.

Organisations solely handling such information may choose to have regard to this code of practice but are not obliged to by the Health and Social Care Act 2012.

What is confidential information?

The legal definition of confidential information for the purposes of this code of practice is broad. It includes matters that many people would not consider to be private or sensitive. Confidential information is:

1. Information which is in a form which identifies any individual to whom the information relates or enables the identity of such an individual to be ascertained, or
2. Any other information in respect of which the person who holds it owes an obligation of confidence.[d]

As a result, for the purposes of this code of practice, information is either confidential information or it is not. The definition of confidential information is illustrated in Figure A on page 8.

Information identifying a person may include information publicly available, for example in telephone directories or public registers. In such cases, when connected with the provision of health services or adult social care, this information becomes confidential information.

Information held under an obligation of confidence may include commercial information, management information, intellectual property, information concerning an individual after death or an unborn child.

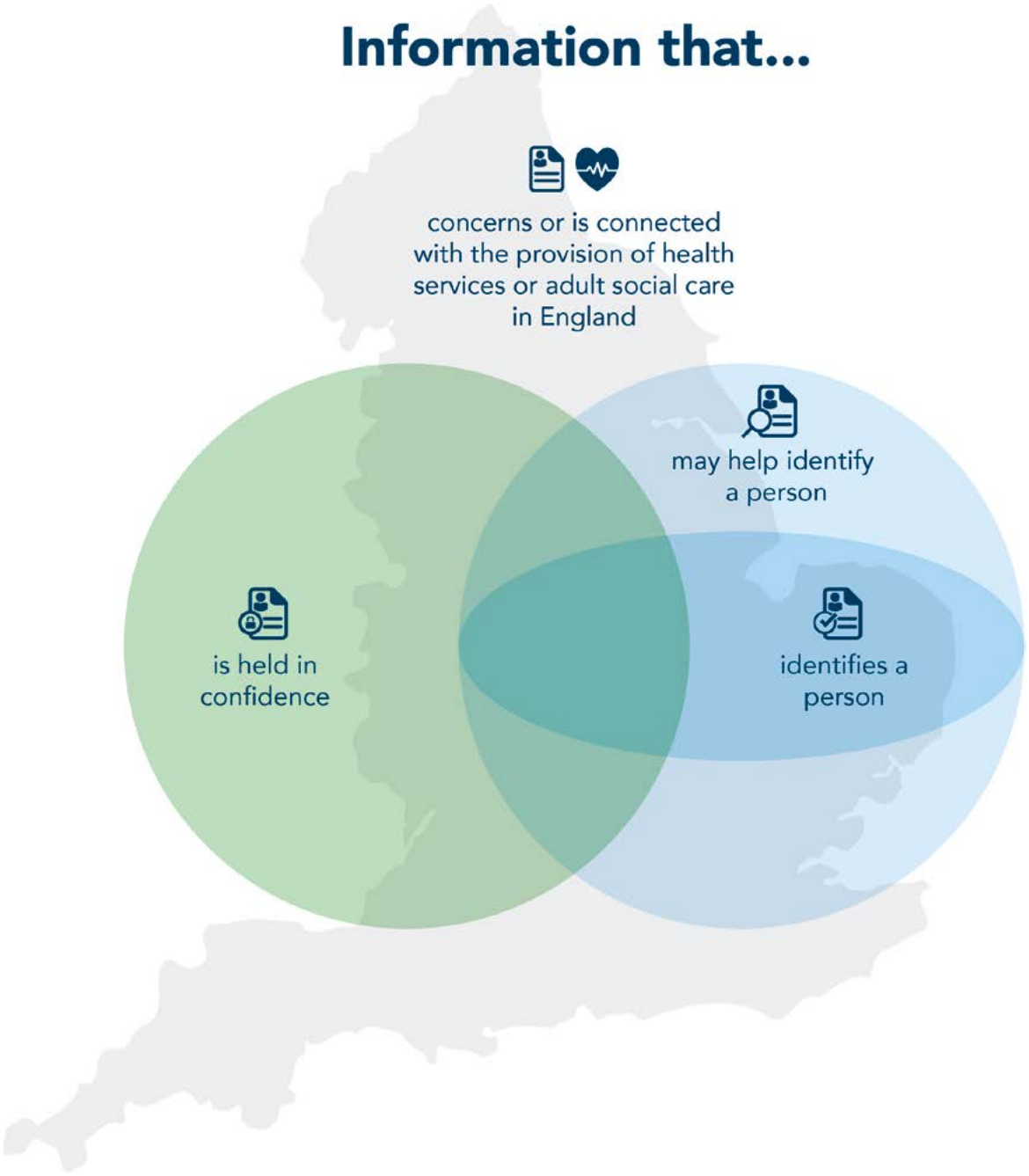


Figure A – Definition of confidential information in scope for the code of practice on confidential information

Review and revision

The Health and Social Care Information Centre **must**[e] keep the code of practice under review and may revise it as it considers appropriate. Review is expected to take place at least annually as well as following any relevant changes in law.

Review may also take place once additional good practices have been determined. It is anticipated that practices concerning pseudonymisation and practices concerning the recording and handling of objections to the use and sharing of person identifiable data will be included in a future revision.

Document structure

This code of practice is structured around a series of information-handling activities as shown in Figure B - Activities in the information-handling life cycle on page 9.

These activities are ordered to follow the life cycle of information-handling from the intent to process a type of confidential information, through establishing and implementing systems to process it, to the eventual destruction of the collected confidential information.

Caldicott principles

Relevant Caldicott principles are shown throughout the document.

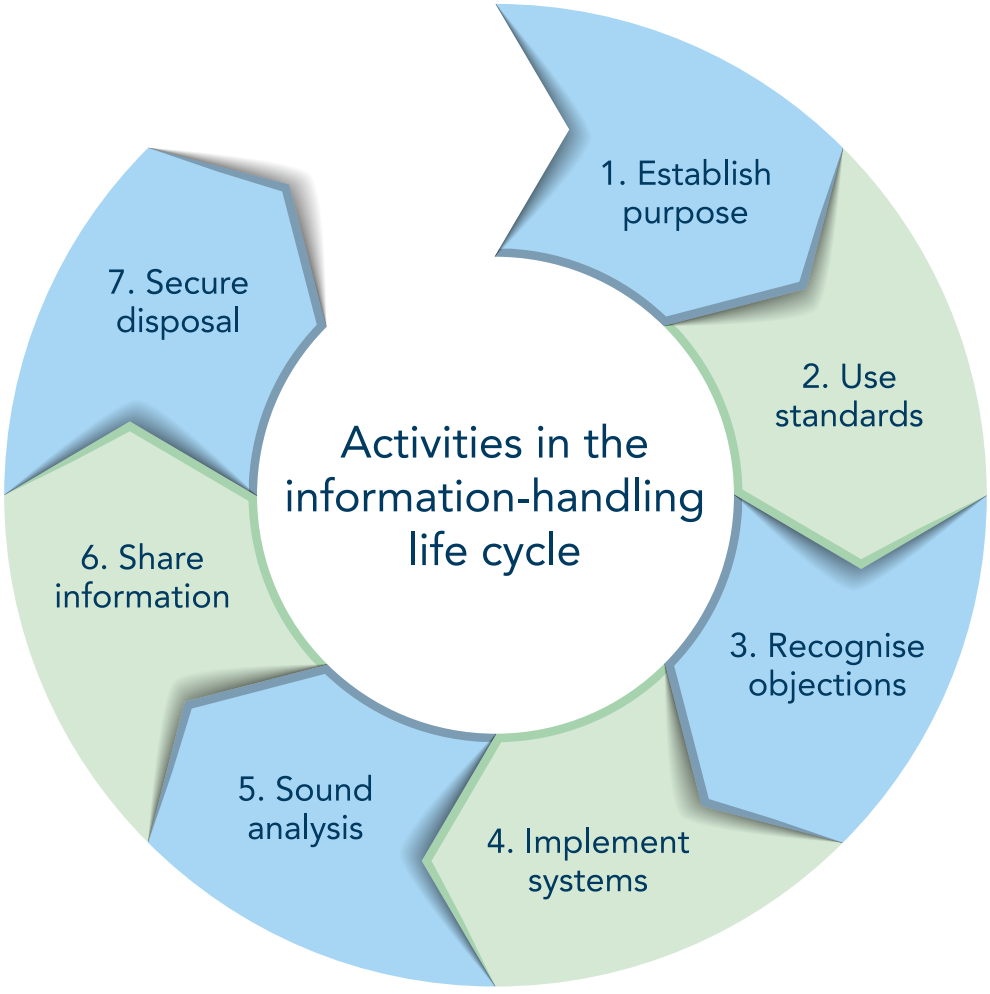


Figure B – Activities in the information-handling life cycle

We have provided annexes with informative flow charts to help determine whether there is an obligation to have regard to this code of practice, details of the standard burden assessment methodology and references to supplementary reading material.

Requirement levels

Each requirement in this code of practice is numbered and states the type of organisations that must have regard to the requirement.

The word **must** is used in this document to identify a legal requirement.

The word **should** is used to indicate that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

The word **may** is used to indicate a truly optional activity. This includes decisions where a permissive legal power is available.

Establish the purpose of arrangements to handle confidential information

Before confidential information is handled, the purpose needs to be understood in detail. Purposes may be for managing the delivery of care for a population, research or another purpose.

1. Organisations seeking to handle confidential information **should** define and describe the intended purpose(s) of handling that confidential information.
2. In addition, organisations seeking to handle data relating to an individual who can be identified **must**[f] define and describe the intended purpose(s) of handling that data.

The Health and Social Care Information Centre can only use its general dissemination powers where the intended purpose is in connection with the provision of health care or adult social care, or the promotion of health. This encompasses a wide range of health and care related intended purposes – including for the commissioning of those services, and the epidemiological research that is needed at the earlier stages of developing new treatments – but not for solely commercial intended purposes such as for commercial insurance.

3. Organisations seeking to handle confidential information **should** assess the impact of handling that confidential information on privacy.[4]
4. Organisations seeking to handle confidential information **should** assess the availability and quality of information and whether that information will meet the intended purpose.
5. Organisations seeking to handle confidential information **should** inform individuals and organisations about the proposed uses of their personal information.
6. A research study **should** adhere to the Research Governance Framework for England.[5]

4 Further information is available from the Information Commissioner's Office at: https://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

5 www.gov.uk/government/publications/research-governance-framework-for-health-and-social-care-second-edition

Caldicott 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.

Caldicott principle 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.

Establish and use standards for handling data

For data to be informative its provenance, structure and meaning need to be understood by all parties handling it. Misunderstanding of these qualities of data is likely to lead to incorrect and inconsistent interpretation and consequent harm.

7. Any organisations seeking to handle confidential information **should** describe the structure and definition of data they are seeking to collect and the means of collection from health or social care bodies (or those providing health or social care as part of an arrangement with a public body).
8. The means of collecting confidential information **should**:
    a. be designed to minimise the risk of a breach of confidence, for example by using anonymised or pseudonymised data where practical
    b. be designed to ensure the quality of data collected is sufficient for the intended purpose(s)
    c. be optimised for handling the collected data
    d. use relevant information standards published by Department of Health or NHS England, and
    e. use relevant data collection specifications published by the Health and Social Care Information Centre.
9. Where there is a requirement for new or changed information standards or specifications these **should** be assured using the same means as Department of Health, NHS England and the Health and Social Care Information Centre.

Transcription

Transcribing data from one form to another, either manually or by computer, may increase costs and reduce the quality and usefulness of that data.

10. Organisations collecting confidential information **should** design collection systems which avoid requirements for transcribing data.

Example of practice: systems to avoid transcription

When Moorfields Eye Hospital established a virtual clinic service for patients with glaucoma they chose to avoid the transcribing of data by adopting messages conforming to the Clinical Document Architecture specification.

These structured messages, generated from care records managed in the iRIS iPad application at remote clinics in England and Wales, are sent over the N3 Network directly into the OpenEyes paperless electronic patient record system.

The patient records are reviewed in a virtual clinic by staff at Moorfields.

Single source of information standards and data collection specifications

Organisations need access to an appropriate single source of guidance to help the health service and adult social care in England to apply consistent information standards and data collection specifications.

The Health and Social Care Information Centre maintains[9] a register of all information it obtains as a result of requests made by national and other bodies.

The Health and Social Care Information Centre maintains a single public register of information standards and data collection specifications including:

a. all information standards published by Department of Health and NHS England

b. all data collection specifications specified by the Health and Social Care Information Centre

c. information standards and data collection specifications assured using the same means as Department of Health, NHS England and Health and Social Care Information Centre

d. relevant National or International Standards, and

e. other relevant information standards and data collection specifications developed elsewhere.

Recognising objections to the handling of confidential information

Individuals' objections to the handling of information about them

The NHS Constitution pledges that "where a patient's identifiable information has to be used, patients are given the chance to object wherever possible"and that patients have the right "to have objections considered, and where patients' wishes cannot be followed, to be told the reasons including the legal basis".

An individual may express an objection to uses of his/her information. Such objections may limit the use of his/her information for certain purposes. However, there are other purposes for which an individual does not have a right to prevent data about them being used, for example, the use of personal data to prevent the spread of infection of notifiable diseases and to prevent further outbreaks in future.

11. Organisations **should** take appropriate steps to notify individuals of the circumstances in which and means by which they are able to object to ongoing and future uses of their confidential information and the circumstances under which an objection cannot be upheld.
12. Organisations handling confidential information **should** implement appropriate procedures for recognising and responding to individuals' requests for access to their personal data.
13. Where an individual objects to the use of confidential information identifying him/her for purposes which are only permitted but are not required by law, organisations **should** act in accordance with that objection.
14. Organisations recording confidential information **should**:
    a. record objections to the handling of confidential information made by data subjects and
    b. notify the recipients of shared confidential information about:
        i. records containing confidential information where the data subject expresses an objection to information leaving that receiving organisation
        ii. records containing confidential information where the data subject withdraws an objection to that information leaving that receiving organisation, and
        iii. the number of records which have not been shared respecting data subjects' objections.

Information held under an obligation of confidence

15. The permitted and non-permitted purposes for the disclosure and receipt of confidential information that is not about an individual **should** be set out in a data transfer contract or agreement. See 'Restricted sharing of information' on page 21.

Implement systems for handling confidential information

The arrangements and infrastructure for handling confidential information need to maximise the benefit gained from that information while minimising the risk of a breach of confidence and remaining effective, efficient and economic. Such arrangements and infrastructure are as much about how the people doing the work are trained to behave as they are about the technology they use. Both aspects need to be established and assured before confidential information is collected.

Efficient systems

The Health and Social Care Information Centre has discretion to provide advice on issues related to the handling of information. This is intended to help minimise duplication and burdens relating to information collection.

16. The Health and Social Care Information Centre **may**[h] provide advice to certain persons who are handling confidential information, including the Secretary of State, any health or social care body, and any person who collects information relating to the provision of health care or adult social care in order to describe how to minimise the burden they impose on other organisations handling confidential information. The Health and Social Care Information Centre **may** undertake a burden assessment in order to prepare that advice.
17. A health or social care body to whom advice is given under section 265 of the Health and Social Care Act 2012 **must**[i] have regard to the advice or guidance concerning the handling of confidential information provided by the Health and Social Care Information Centre.
18. A registered person **must** have regard to guidance published by NHS England on the practice to be followed by them in relation to the processing of:
    a. patient information, and
    b. any other information obtained or generated in the course of the provision of the health service.

The Health and Social Care Information Centre publishes and uses a standard burden calculation methodology included in Annex 3 – Burden on page 31.

At least once every three years at the request of the Secretary of State the Health and Social Care Information Centre gives[j] advice about how the burdens relating to the collection of information imposed on health or social care bodies may be minimised.

19. All organisations seeking to request or require a collection of confidential information from other organisations **may** seek advice from the Health and Social Care Information Centre on how the burdens relating to the collection of confidential information imposed on health or social care bodies may be minimised.
20. Any organisation **may** provide details of a data collection using or derived from confidential information to the Health and Social Care Information Centre so that data collection may be included in the assessment of burdens relating to the collection of information imposed on health or social care bodies.

Safe systems

21. Information about an individual which is held in confidence **must not** be disclosed to a third party unless:
    a. the person that the information is about has consented, or
    b. there is a statutory basis for disclosure or court order, or
    c. there is a public interest justification for disclosure,[6,7] or
    d. there is another basis in law for disclosure.

Caldicott principle 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.

22. Organisations holding confidential information for different purposes should take steps to avoid intentional or unintentional linkage unless:
    a. the person that the information is about has consented, or
    b. there is a statutory basis for disclosure or court order, or
    c. the relevant public interest test is satisfied, or
    d. there is another basis in law for linkage.

Example of practice: publishing confidential information where there is a public interest justification for disclosure

NHS Choices includes links to information about individual consultants in a number of clinical areas[8]. Patients can look at their results for a range of operations and treatments to help them make decisions about their care. The data show where the clinical outcomes for each consultant sit against the national average. Putting this information into the public domain can help drive up standards.

Guidance is available concerning whether a relevant public interest justifies disclosure in particular circumstances.

- The Department of Health has published Confidentiality: NHS Code of Practice Supplementary Guidance: Public Interest Disclosures[9].

6 Further information is available in Confidentiality: NHS Code of Practice Supplementary Guidance on Public Interest Disclosures at www.gov.uk/government/publications/confidentiality-nhs-code-of-practice-supplementary-guidance-public-interest-disclosures
7 Handbook to the NHS Constitution available at: www.nhs.uk/choiceintheNHS/Rightsandpledges/NHSConstitution/Pages/Overview.aspx
8 www.nhs.uk/choiceinthenhs/yourchoices/consultant-choice/pages/consultant-data.aspx
9 www.gov.uk/government/publications/confidentiality-nhs-code-of-practice-supplementary-guidance-public-interest-disclosures

- The General Medical Council has published Confidentiality[10] which sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow.
- The Information Commisisoner's Office has published Conducting privacy impact assessments code of practice[11] which sets out the basic steps which an organisation should carry out during the privacy impact assessment process.

Management systems

23. Organisations handling confidential information **should**:
    a. Define and implement comprehensive policies for the management of confidential information with required strategies and/or improvement plans.*
    b. Provide staff with awareness and training in the correct handling of confidential information.*
    c. Access the confidentiality, information security and data protection skills, knowledge and experience necessary to meet the organisation's assessed needs.
    d. Establish and implement appropriate audit procedures to monitor access to confidential information.
    e. Document, implement and review a formal information security risk assessment and management programme for key Information Assets.
    f. Document, adopt and review an information risk policy and information risk management strategy covering the handling of confidential information. These should be owned by a Senior Information Risk Owner with appropriate support.
    g. Adopt formal contractual arrangements with all contractors and support organisations that include compliance with requirements for the handling of confidential information.
    h. Adopt employment contracts with all staff handling confidential information on behalf of the organisation. These contracts should include compliance with requirements for handling confidential information.

***Caldicott principle 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.

24. Organisations handling confidential information **should**:
    a. adopt management systems for their quality and security management, and
    b. publish at least once in any three-year period a statement indicating the extent to which these management systems conform to:
        i. a quality management system standard equivalent to ISO 9001:2008,[12] and
        ii. an information security management system standard equivalent to ISO/IEC 27001:2013.[13]

10 www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp
11 www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment
12 www.iso.org/iso/catalogue_detail?csnumber=46486
13 www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Supplying confidential information to the Health and Social Care Information Centre

The Health and Social Care Information Centre has powers to require or request provision of information needed for the functions it exercises.

25. All health or social care bodies **must**[k] supply the Health and Social Care Information Centre with confidential information required under these powers except where:
    a. an individual has objected to his/her information leaving the health or social care delivery organisation, and
    b. there is a legal requirement to respect that objection such as the terms of a related direction to the Health and Social Care Information Centre.[l]

26. Providers of health services or adult social care **must not**[m] provide false or misleading information required to be provided by regulations under an enactment or other legal obligation.

Handling confidential information

27. All organisations handling confidential information **should**:
    a. Minimise the risk of a breach of confidence.
    b. Use industry standard encryption.
    c. Hold anonymised or pseudonymised data in preference to retaining the identity of the subject of that information where practical.
    d. Document, implement and review information security incident/event reporting and management procedures that are used by all staff handling confidential information.
    e. Implement appropriate access control functionality with documented and managed access rights for all users of systems handling confidential information.
    f. Have and use a capability for the rapid detection, isolation and removal of malicious code and unauthorised mobile code affecting confidential information.
    g. Implement secure Information Communication Technology networks for handling confidential information.
    h. Establish adequate safeguards to ensure that all confidential information is collected and used within a secure data processing environment (safe haven) distinct from other areas of organisational activity.

Caldicott principle 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).

Caldicott principle 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.

Example of practice: sharing confidential information by e-mail

Local safeguarding boards depend on sharing confidential information such as board papers and minutes. These are shared between board members by using secure e-mail. NHS organisations use NHSMail and connect with partners including the police and local authorities using the Government Secure Intranet.

Adopt sound analysis of confidential data

Analysis of data includes the processes of inspecting, cleaning, linking, transforming, modelling and visualising data with the goal of discovering useful information, reasoning, suggesting conclusions and supporting decision-making.

28. Quality **should** be monitored, assured and reported on, taking account of internationally agreed practices, for example the European Statistical System dimensions of quality.[14]

29. An organisation undertaking analysis of data for publication or other dissemination **should**:

    a. Ensure that analyses, findings, statistics and conclusions are produced according to scientific principles.

    b. Publish details of the methods adopted, including explanations of why particular choices were made.

    c. Ensure that analyses, findings, statistics and conclusions are produced to a level of quality that meets users' needs, and that users are informed about the quality of publications.

    d. Adopt quality assurance procedures, including the consideration of each product against users' requirements, and of their coherence with other statistical products.

14 These dimensions are relevance, accuracy, timeliness and punctuality, accessibility and clarity, comparability and coherence

e. Publish quality guidelines, and ensure that staff are suitably trained in quality management.

f. Seek to achieve continuous improvement in analysis and statistical processes by, for example, undertaking regular reviews or releasing work in progress such as experimental statistics.

g. Promote comparability within the UK and internationally by, for example, adopting common standards, concepts, sampling frames, questions, definitions, statistical units and classifications (including common geographic referencing and coding standards).

h. Make the reasons for any deviations from standard models publicly available, and

i. Produce consistent historical data where time series are revised or changes are made to methods or coverage.

Share information

The maximum value is gained from information when it is used to make sound decisions. Sharing or disclosure of information or making it public where this does not breach confidentiality enables the value of the information to be harnessed.

Sharing occurs whenever one entity with control over confidential information transfers or permits access to data, or grants control of data by another entity. The new entity commonly will gain with control over confidential information although it may also be a processor of data acting under instruction from the entity controlling the information. It also includes sharing as a part of planning and delivering care (such as supporting requests, referrals or handover) or sharing for any other purpose.

Caldicott principle 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.

Caldicott principle 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.

30. All arrangements for sharing of confidential information **must** be lawful.[15]

31. All organisations **should** be able to demonstrate that their arrangements for sharing of confidential information are lawful.

15 Some of the key legal requirements include the Data Protection Act 1998, the Human Rights Act 1998 and the common law of confidentiality

32. All organisations sharing confidential information **should** hold, maintain and publish a data release register.
33. The legal arrangements for sharing confidential information **should** be included in that data release register.
34. All arrangements for sharing of confidential information should have regard to:
    a. an assessment of the impact of the sharing of confidential information on privacy
    b. the Anonymisation Standard for Publishing Health and Social Care Data[16]
    c. the Data Sharing Code of Practice,[17] and
    d. Anonymisation: Managing Data Protection Risk Code of Practice[18] published by the Information Commissioner's Office.

Sharing by publication

A publication is a planned release of a defined set of information made generally available. Publications may include textual commentary to explain and interpret the information or a range of summary information and may provide these and detailed information in a wide range of formats to suit different user needs.

35. Where the purpose for handling confidential information is research, analyses, findings and publications that do not include confidential information but were created using confidential information **should** be made openly available with immediate, unrestricted, on-line access, free of any access charge and with maximum opportunities for re-use.
36. Such analyses, findings and publications **should** be published using either the Open Government Licence where the publisher is a public body, the Creative Commons Attribution (CC BY) licence or equivalent.

The Health and Social Care Information Centre **must not** publish information which identifies or enables the identity of an individual to be ascertained,[n] except it has a discretion as to whether to publish information which identifies a person who provides health care or adult social care or a body corporate who does so.[o] For all other information collected following a direction or request, the Health and Social Care Information Centre is required to publish that information.

Official Statistics

A publication is deemed Official Statistics if it is produced by a body listed in the annual Official Statistics Order, and is

a. national in scope
b. repeated or likely to be repeated
c. produced using reputable methods, and
d. likely to excite the public interest.

37. Official Statistics **must**[p] be produced and published in compliance with the Code of Practice for Official Statistics[19], and with the Pre-release Access to Official Statistics Order (2008), and have regard to guidance issued from time to time by the National Statistician.

16 www.isb.nhs.uk/library/standard/128
17 www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing
18 www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation
19 www.statisticsauthority.gov.uk/assessment/code-of-practice/

38. Production and publication of Official Statistics **must**[p] be demonstrably separated from the political process, in accordance with the Code of Practice for Official Statistics.

Other publications

39. Any political involvement or other interest in the production or release of other publications **should** be declared in the publication.

Restricted sharing of information

There are circumstances where it is not permissible to make information publicly available, however it may be permissible and appropriate to share that information with other organisations so that they may make reasonable use of it. Such restricted sharing of information may include sharing information to support the delivery of care for individuals, for managing systems of care for a population or for other purposes.

40. Under common law, any restricted sharing of information must not identify any individual unless there is a legal means and purpose to do so. Permissible legal means will include cases when:
    a. the person that the information is about has consented, or
    b. there is a statutory basis for disclosure or court order, or
    c. there is a public interest justification for disclosure, or
    d. there is another basis in law for disclosure.

Example of practice: Children of the '90s

The Avon Longitudinal Study of Parents and Children study (ALSPAC, also known as 'Children of the 90s') recruited over 14,000 pregnant women between 1991-92 and has followed up the mothers, children and partners intensively since then, collecting large amounts of health, biomedical and genetic data and samples. Over 1,000 academic papers have been published as a result of information supplied by Children of the '90s participants.

Through the Project to Enhance ALSPAC through Record Linkage (PEARL), the study has provided fair processing information to the index children informing them of the study's intention to collect information from health and administrative routine records.

Through consent, or with support from the Secretary of State for Health through the 'Section 251' regulations, ALSPAC has linked individual participants to the Hospital Episode Statistics data from the Health and Social Care Information Centre. Using this link ALSPAC has extracted Hospital Episode Statistics data and has identified participants' registered GP practices. Through general practice software companies PEARL has extracted data from primary care records into a Farr Institute Safe Haven. ALSPAC is also undertaking linkages with other data such as education records.

ALSPAC has significantly improved its practice with regard to the management of confidential participant information in recent years, gaining ISO 27001 certification in 2012 and NHS Information Governance Toolkit compliance in 2014.

41. Organisations **should** only make confidential information available under terms defined in a data sharing contract or agreement for specific purpose(s). Such a contract or agreement will not in itself provide a legal basis but should specify the legal basis.

A contract is required where the recipient is not a public body. An agreement will apply between NHS bodies and may be applicable between public bodies.

42. Prior to entering into a data sharing contract or agreement for specific purposes the organisation seeking to disseminate confidential information:
    a. **should** assess the availability and quality of information and whether that information will meet the intended purpose stated by the proposed recipient (see Establish the purpose of arrangements to handle confidential information on page 10), and
    b. **should** review and understand what steps have been established by the proposed recipient to avoid data linkage, unless the data linkage is necessary to achieve the intended purpose and one or more of the following applies:
        i. the person that the information is about has consented, or
        ii. there is a statutory basis for data linkage, or
        iii. there is a public interest justification for data linkage, or
        iv. there is another basis in law for data linkage.
43. A data sharing contract or agreement **should** include:
    a. the legal basis for disclosure and use
    b. permitted purposes and manners in which the data will be processed
    c. whether onward sharing is permitted and on what terms
    d. arrangements for data destruction once the specified purpose(s) are achieved (see Dispose of information once it is no longer required on page 24)
    e. provision for audit of adherence to the contract and/or agreement
    f. arrangements for data destruction if the terms of the contract or agreement are broken
    g. penalties if the terms of the contract or agreement are broken
    h. research publication licence rights (see Sharing by publication on page 20), and
    i. permitted arrangements for linkage to other sources of data.

Further guidance on arrangements for data sharing are provided in the statutory data sharing code of practice[20] published by the Information Commissioner's Office.

Receiving information subject to permitted purposes and manners described in a data sharing agreement, but with the freedom to determine the precise purposes for which, or the manners in which, the data will be processed will establish an additional entity with control over confidential information.

44. Each additional entity with control over confidential information **should** advise the other entities with control over confidential information of the precise purposes for which and the manner in which those data will be processed.

20 https://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

Standards and formats

The choice of structure and the representation of the meaning of data can affect its utility or limit the available sources of applications for subsequent handling of data. Using a proprietary format or structure or a code list for which the recipient has restricted rights to use is a barrier to re-use and to maximising the value of confidential information. Proprietary formats may also lead to a dependency on one or more software or service vendors or increase the cost of consuming information.

45. Public bodies **should** make information available as structured data in relevant open formats agreed by the UK Government Open Standards Board[21] or the Standardisation Committee for Care Information.[22]

Data will often include codes or identifiers to assist computation. Without an understanding of the meaning of the code or the item identified by a coded identifier, it is not possible to fully utilise the data. Using a code or identifier which acts as a link to a World Wide Web resource can overcome this barrier.

46. Organisations **should** use resolvable hypertext transfer protocol universal resource locators (http URLs) as identifiers.[23]

47. Organisations **may** additionally make information available in proprietary formats and with other identifiers.

21 HM Government Standards Hub http://standards.data.gov.uk/
22 www.hscic.gov.uk/isce
23 HM Government Open Data Standard – Persistent resolvable identifiers, www.standards.data.gov.uk/profile/persistent-resolvable-identifiers-standards-profile

Dispose of information once it is no longer required

The storage of confidential information inherently leads to a degree of risk of inappropriate sharing. Once the entity with control over confidential information identifies that the confidential information is no longer required, this risk can be mitigated by secure disposal.

48. Entities with control over confidential information **should** dispose of their confidential information once it is not required. A requirement may include retention in accordance with the NHS Retention and Disposal Schedule.

49. Data controllers **must**[q] dispose of personal data once it is not required.

Disposal may be initially logical (retaining data but removing data that enables it to be accessed, putting the data beyond use), but should as soon as possible be physical (destroying all copies of the data using physical means such as media destruction or securely overwriting data).

50. Any health organisation handling confidential information **should** have regard to:

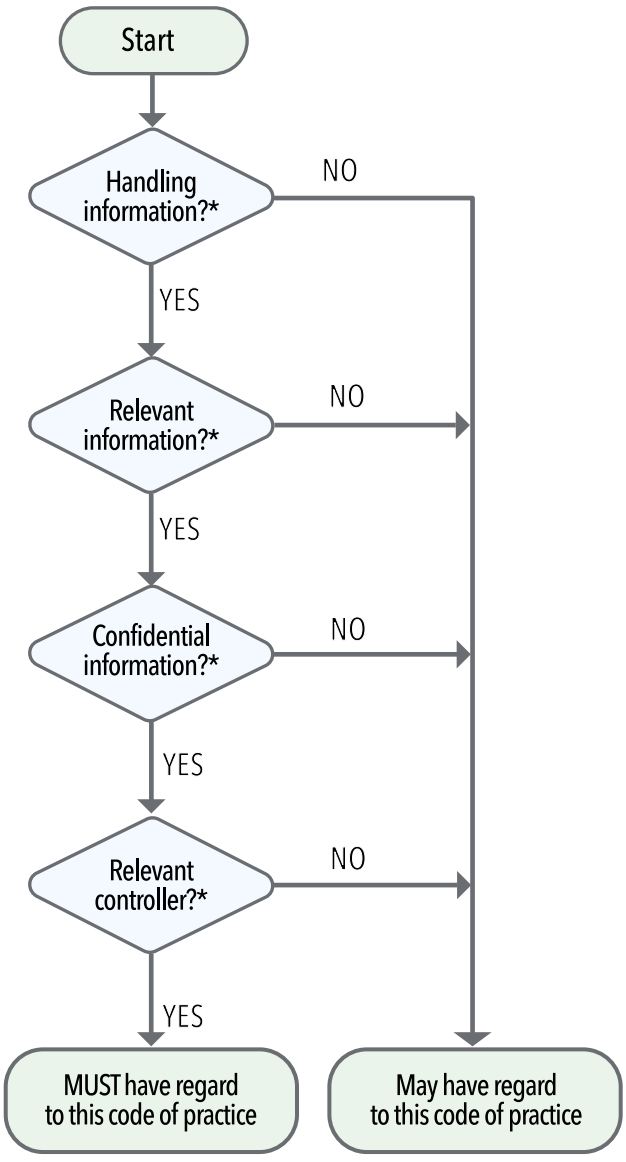
    a. the NHS Retention and Disposal Schedule

    b. NHS Code of Practice on Records Management when considering destruction of any confidential information, and

    c. legal obligations which set minimum retention periods.

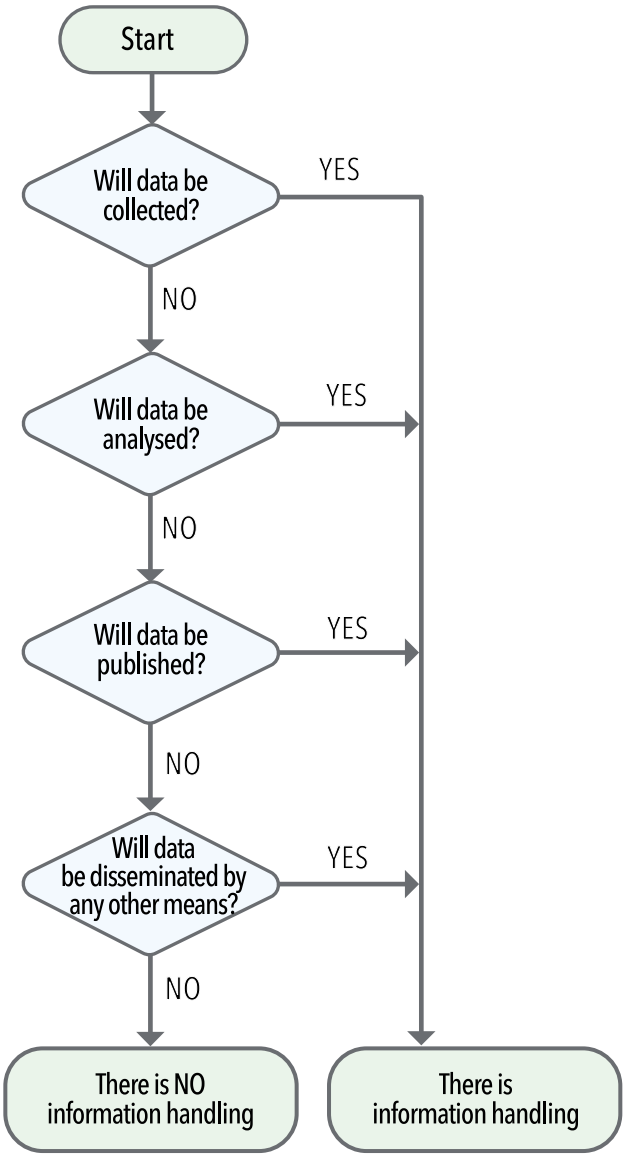
Annex 1 – decision support charts for determining the scope of the code of practice

High level decision support chart for determining the scope of the code of practice

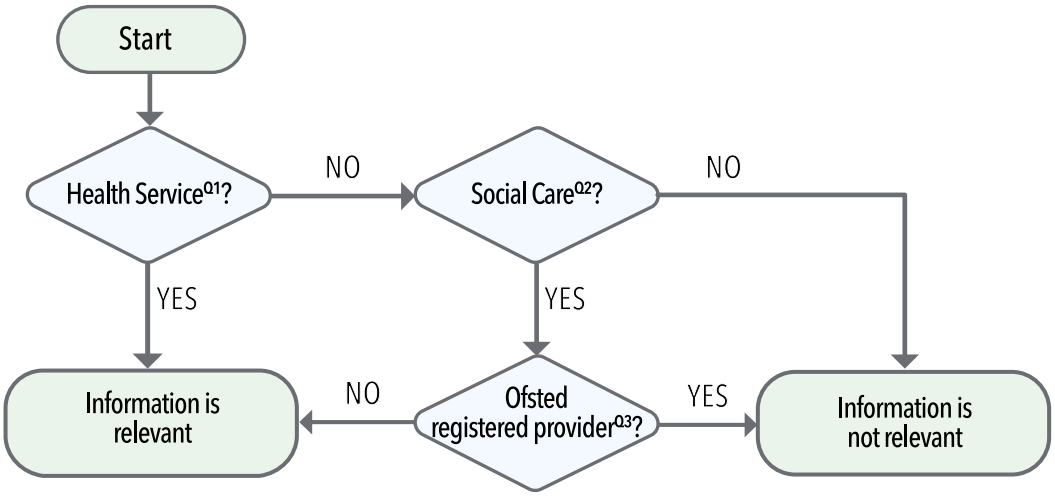


*Each of these four high level decisions are supported by one of the decision support charts on the following pages.

Decision support chart – handling information



Decision support chart – relevant information

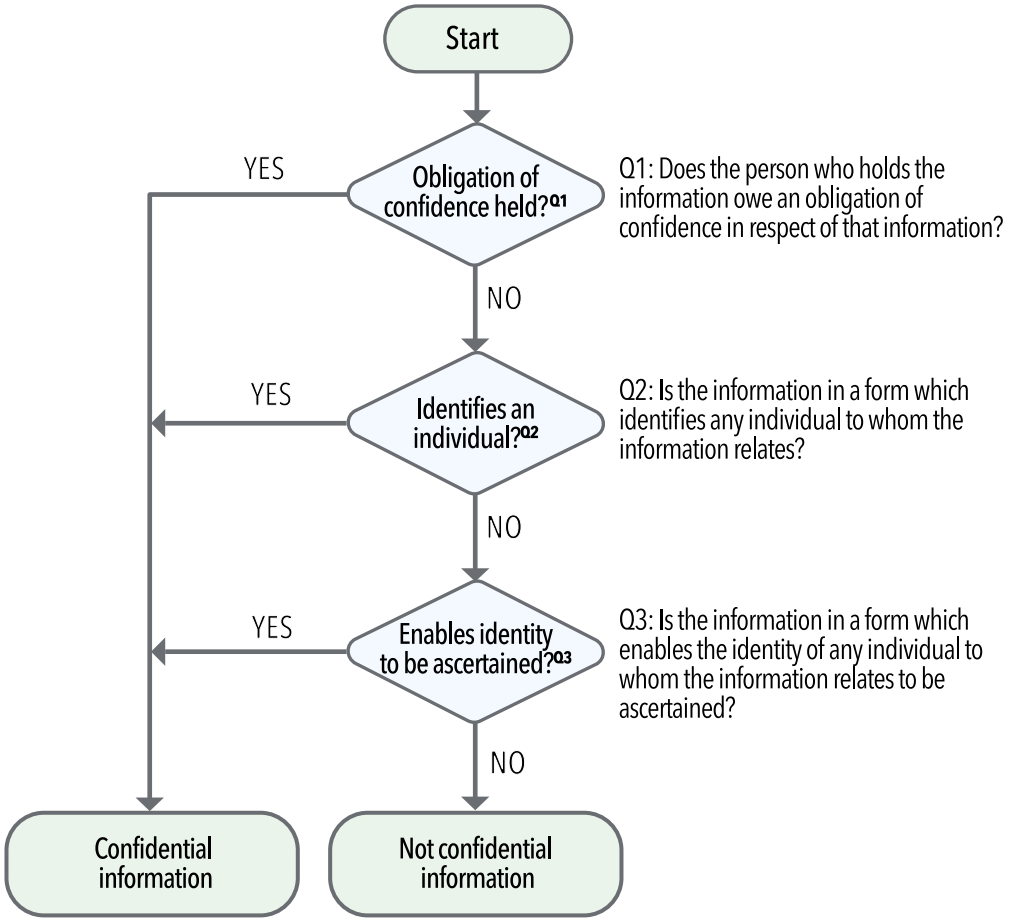


Q1: Is the data concerning or connected with the provision of services which must or may be provided as part of the health service in England?

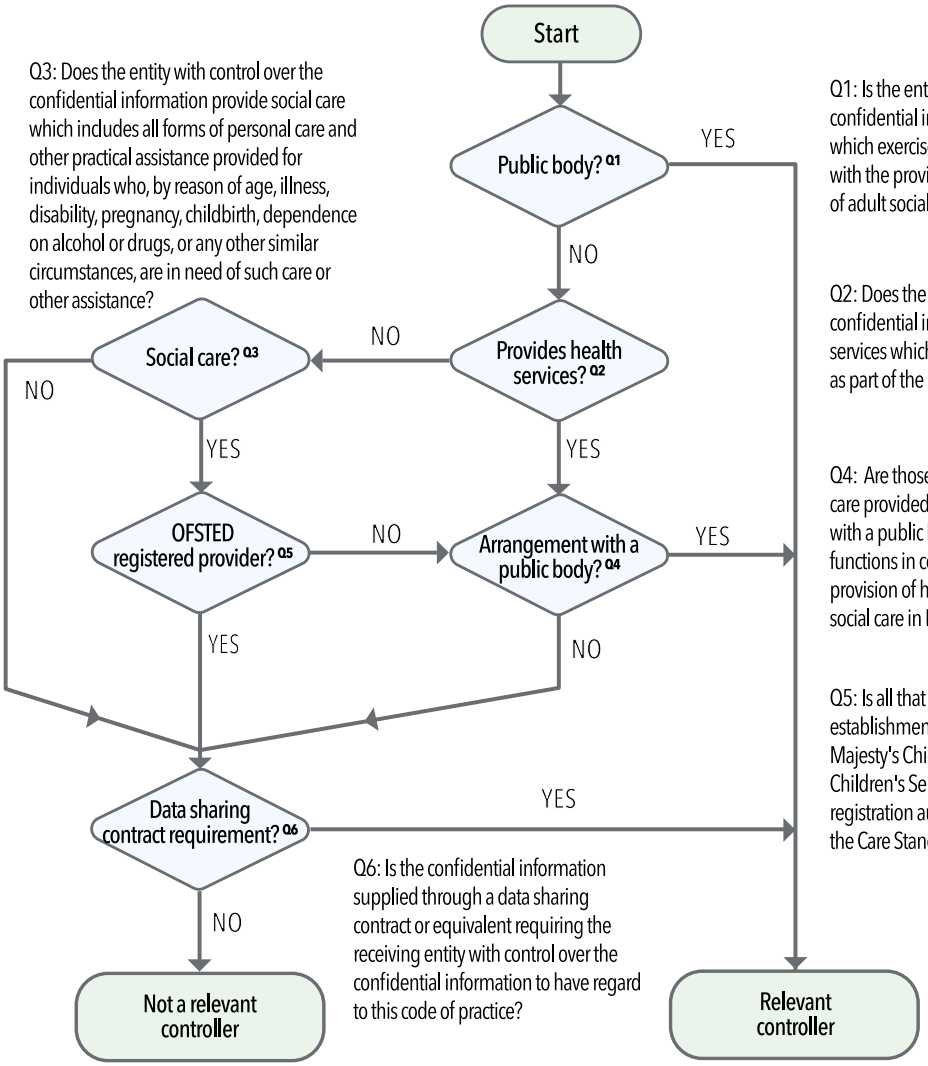
Q2: Is the data concerning or connected with the provision of social care which includes all forms of personal care and other practical assistance provided for individuals who, by reason of age, illness, disability, pregnancy, childbirth, dependence on alcohol or drugs, or any other similar circumstances, are in need of such care or other assistance?

Q3: Is all that social care provided by an establishment or agency for which Her Majesty's Chief Inspector of Education, Children's Services and Skills is the registration authority under section 5 of the Care Standards Act 2000?

Decision support chart – confidential information



Decision support chart – relevant controller



Annex 2 – The Caldicott Principles

Caldicott 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.

Caldicott principle 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).

Caldicott principle 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.

Caldicott principle 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.

Caldicott principle 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.

Caldicott principle 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.

Caldicott principle 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.

Annex 3 – Burden

Burden includes:

- local and national requests. Local requests will be included in the three year review of burden but are not in scope of the burden assessment for new collections.
- regulatory, commissioning and performance management requests
- re-recording data because it is required in a different way
- data sets and audits
- financial, workforce, activity and other information
- mandatory, voluntary or statutory collections
- exception reporting
- data extracts, electronic, telephone and paper returns
- samples (on a case-by-case basis)
- regular and one-off collections
- non-direct care uses, and
- standards.

Burden excludes:

- intra-organisational collections (collections performed internally by organisations).

Definition of burden

Assessed burden is the professional assessment of the time and associated costs incurred by stakeholders in England resulting from the implementation, on-going use and eventual decommissioning of an information standard, data collection or data extract.

This cost assessment includes, but is not limited to:

- collection, validation, extraction, transcription and transmission of data
- analysis, validation, publication, and consumption of data
- storage and destruction of data
- additional care activity (activity undertaken primarily for the collection of data), and
- implementing and maintaining standards.

Burden also includes the cost of:

- developing, implementing, using and decommissioning systems (electronic or other), and
- training and labour.

Burden excludes the cost of:

- self-selected contribution to surveys
- collection of data where the collecting stakeholder currently collects the data as part of routine business e.g. NHS Blood and Transplant collects data to enable patients to be registered for transplantation. These data are collected for routine business and are thus exempt, however if they also asked for eye colour, it would not be routine business and therefore a burden would be incurred.

- responding to complaints
- completing legal reports including coroner's reports
- infrastructure (including any place of work of an NHS employee), and
- care professional contribution to a collection or extraction where the collection or extract uses terms that are described and defined in either a National Institute for Health and Care Excellence Guideline or a professional body Clinical Guideline so long as those terms are part of the approved reference terminology or terminologies for electronic care records in the health and social care system in England. This will ensure that the definition of burden maximises staff time on caring for patients rather than transforming or transcribing data collections.

The assessed burden is not limited to administrative and management activities. For example it will include the cost of any additional investigations not ordinarily performed as part of routine business.

Methodology

Burden = cost of:

collection + validation + extraction + transcription + transmission + analysis + publication + consumption + storage + destruction of data + system development + implementation + use of systems + decommissioning systems + training + labour + infrastructure.

The burden calculation uses the HSCIC median pay report uplifted by a factor of 1.3 for employers National Insurance / pension to produce the burden £. This excludes overhead costs.

Glossary

Some of the definitions used in this glossary have particular meanings in the context of this code of practice and the Health and Social Care Act 2012.

Adult social care – broadly, social care other than Children's social care (see section 253(3) of the Health and Social Care Act 2012).

Anonymised data – data that has been converted into a form that does not identify individuals and where identification is unlikely to take place.

Burden assessment – professional assessment of the time and associated costs incurred by organisations in England resulting from the implementation, on-going use and eventual de-commissioning of an information standard, data collection or data extract.

Children's social care – social care services provided by an Ofsted registered body.

Confidential information – information which is in a form that identifies any individual to whom the information relates or enables the identity of such an individual to be ascertained, or any other information in respect of which the person who holds it owes an obligation of confidence.[r]

Data – reinterpretable representation of information in a formalised manner suitable for communication, interpretation or processing.

Data controller – a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data subject – an individual who is the subject of personal data.

Health services – services which must or may be provided as part of the health service[24] in England.

Information – knowledge concerning objects that within a certain context has a particular meaning.

Personal data – has the meaning given in the Data Protection Act 1998.

Pseudonymised data – data that has been de-identified so that a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without that individual being identified.

Registered person – a person registered under the Health and Social Care Act 2008 Chapter 2 as a manager or service provider in respect of a regulated activity.

Research – the attempt to derive generalisable new knowledge including studies which aim to generate hypotheses as well as studies that aim to test them.[25]

Research study – attempt to derive new knowledge that will have a general application, by addressing clearly defined questions with systematic and rigorous methods.

Social care – all forms of personal care and other practical assistance provided for individuals who, by reason of age, illness, disability, pregnancy, childbirth, dependence on alcohol or drugs, or any other similar circumstances, are in need of such care or other assistance.

Time series – a sequence of observations which are ordered in time.

24 The 'health service' has the same meaning as in the National Health Service Act 2006, which, by section 275(1) of the NHS Act means the health service continued under section 1(1) of the NHS Act and under section 1(1) of the National Health Service (Wales) Act 2006

25 www.hra.nhs.uk/research-community/before-you-apply/determine-whether-your-study-is-research/

Relevant legal bases

[a] Health and Social Care Act 2012 s263(1)

[b] Health and Social Care Act 2012 s263(7)

[c] Health and Social Care Act 2012 s.274(9)

[d] Health and Social Care Act 2012 s.263(2)

[e] Health and Social Care Act 2012 S263(5)

[f] Data Protection Act 1998 Schedule 1, Part 1, Principle 2 and common law duty of confidence

[g] Health and Social Care Act 2012 s.264

[h] Health and Social Care Act 2012 s.265 (1) and (2)

[i] Health and Social Care Act 2012 s.265(5)

[j] Health and Social Care Act 2012 s.265(3)

[k] Health and Social Care Act 2012 s259

[l] Health and Social Care Act 2012 s254

[m] Care Act 2014 s92

[n] Health and Social Care Act 2012 section 260 (2)

[o] Health and Social Care Act 2012 section 260 (3)

[p] Code of Practice for Official Statistics 2009

[q] Data Protection Act 1998 Schedule 1, Part 1, Principle 5

[r] Health and Social Care Act 2012 s263(2)

Code of practice on confidential information

Published by the Health and Social Care Information Centre

Version 1.0
December 2014

www.hscic.gov.uk

The HSCIC is committed to building on this code of practice and updating it regularly, working with partners such as the Information Governance Alliance, and drawing on the experience of other organisations and sharing their practical examples of practice.
To provide feedback on this code of practice:

Tel: 0845 371 3671
Email: exeter.helpdesk@hscic.gov.uk