hscic Health & Social Care Information Centre

# A guide to confidentiality in health and social care

## Treating confidential information with respect

# A guide to confidentiality in health and social care

Published by the Health and Social Care Information Centre

## Version 1.1

September 2013

# Contents



# Foreword

**Health and social care is being transformed so that each individual can have greater control of their own care. There has been an explosion of information produced by the increase in internet use, social media and electronic information systems and we want patients and service users to be able to take advantage of this. This makes protecting confidential information the starting point, if people and professionals are to feel confident about the security and appropriateness of information sharing.**

For too long, people have hidden behind the obscurity of the Data Protection Act or alleged rules of information governance in order to avoid taking decisions that benefit the service user or patient. I was asked by the Secretary of State to review the balance between confidentiality and information sharing in this context. My panel's report has reinforced the duty of staff to share information to ensure safe and effective care for service users and patients.

We are equally committed to ensuring that the patient or service users' wishes are respected in relation to how their information is used. While people are unlikely to object to sharing confidential information within their own care team, there are some who may not want it used for purposes such as research or reshaping a patient pathway in order to achieve safer care in general. These wishes must be respected by everyone who has access to health and social care data. This guide supports the individual's right to object and sets out how organisations should respect this.

We want to make sure that people have no surprises about how information about them is used. The following guide to confidentiality shows how to ensure this happens. It has been distilled into five rules which set out all the obligations to be fulfilled. We expect it to become part of the DNA for all staff in residential homes, providing care at home, working in wards and in communities. The guide is a living document which we will keep updated to reflect changes in health and social care that have consequences for how information is handled. Individuals should be reassured by this guide and its commitment to ensuring that information is shared for safe and effective care while their privacy and confidentiality is protected.

**Dame Fiona Caldicott**
Chair of the Information Governance Review – To Share or Not to Share?

**Kingsley Manning**
Chair, Health and Social Care Information Centre

# Introduction

## Why has this guide been produced?

Everyone using health and social care services in England is entitled to expect that information they entrust to care providers will be treated in strictest confidence. The promise of confidentiality has been a cornerstone of medical practice for centuries and the relationship of trust between a doctor and patient depends on it. The patient needs to be able to tell the truth about intimate matters, knowing that this information will not be improperly disclosed. This is equally important in social care, for example when a social worker is making arrangements for an individual's care and wellbeing.

People using services deserve a lot more than just information security. Individuals need the teams of professionals who are responsible for their care to share information reliably and effectively. Confidential information about an individual must not leak outside the care team, but it must be shared within it in order to provide a seamless, integrated service.

The community can also derive huge benefits from information that has been collected by health and social care services once it has been anonymised to stop any individual being identified. Advances in medical research and improvements in the design of care services depend on making good use of anonymised information. The Health and Social Care Information Centre (HSCIC) plays a leading role in ensuring that information can be used for community benefit.

Confidentiality, information sharing and community benefit are well established throughout health and social care services in England. Although the concepts are straightforward and little contested, they give rise to complex ethical and administrative problems when put into operation. The subject was examined in depth by the Information Governance Review led by Dame Fiona Caldicott, which reported in April 2013[1]. It set out seven principles to guide decisions about confidential information (Appendix 1) and made a range of recommendations which were accepted by the government in September 2013. This guide reflects these principles throughout and incorporates the good practice outlined by the Information Governance Review.

The HSCIC has a big part to play in implementing these recommendations and will support and assist health and social care organisations in doing so. It also has statutory responsibility under the Health and Social Care Act 2012 to produce a Code of Practice for processing confidential information covering 'the practice to be followed in relation to the collection, analysis, publication and other dissemination of confidential information concerning, or connected with the provision of health services or of adult social care in England.'

1 Further details are available in section 1 ('The Information Governance Review') of the references document available at www.hscic.gov.uk/confguideorg

While preparing that code, the HSCIC heard from many stakeholders that there was also an urgent need for a clear guide to processing confidential information about an individual's care. Importantly, this should be a guide that can be understood by service users, patients, carers, relatives and staff – all of whom need to know what to expect when confidential information is given and received.

The guide needed to focus specifically on what the Information Governance Review termed 'personal confidential data (PCD)'. This is identifiable information about an individual that they would reasonably expect to be held confidentially. The terms 'confidential information' and 'personal confidential information' are used interchangeably in this guide.

This guide has been issued through the HSCIC's powers to provide advice and guidance 'on any matter relating to the collection, analysis, publication or other dissemination of information'[2]. Therefore health and social care bodies (or anyone working with them to provide services or care) processing confidential information in relation to the provision of publicly funded health or adult social care activities, must have regard to this guide.

The guide has been designed to be easily accessible and to de-mystify some of the complexities of the laws, principles and obligations that have sometimes got in the way of good decision making in the past. It brings together the array of overlapping ethical and professional principles and laws in relation to using or sharing confidential information. Ethical principles outline the fundamental standards of behaviour expected of health and social care staff. Professional obligations are set by professional regulators and neglecting them can have severe repercussions for staff, such as being struck off the professional register and not being able to practise their profession again. The law sets out duties which are a mix of the decisions of the courts (known as the 'common law duty of confidentiality'[3]) and legislation such as the Data Protection Act[4] and the Human Rights Act[5].

Together, ethical principles and professional obligations have evolved from moral judgement about what is right and wrong. Some of these considerations are so important that they have been enshrined in law. The confidentiality rules within the guide reflect these considerations so that in most cases, readers do not have to consult multiple sources of guidance. That is not to say that it is always easy to discern what is right. Decisions around sharing confidential information are often not clear cut and require consideration of a balance of interests – those of the individual and the community. This guide aims to enable staff to use their professional judgement confidently in the best interests of the individual and the community.

2 Section 265 of the Health and Social Care Act 2012

3 Further details are available in section 2 ('The common law of confidentiality and consent') of the references document available at www.hscic.gov.uk/confguideorg

4 Further details are available in section 3 ('The Data Protection Act 1998') of the references document available at www.hscic.gov.uk/confguideorg

5 Further details are available in section 4 ('Human Rights Act provisions') of the references document available at www.hscic.gov.uk/confguideorg

# Who needs to know about this guide?

We all do. Confidentiality is too important a subject to be delegated to the few experts who have taken the trouble to master the laws and customs that underpin it. Across England, more than a million people a day make contact with health and social care services, expecting that they can trust the professionals looking after them with confidential information.

Unless those patients and service users understand how confidential information about them will be used and who will get to see it, they cannot be considered to be fully informed when they consent to treatment or care.

And unless members of staff understand when they must share information with another professional and when they should not, they will not be able to provide the optimum standard of care. Lives may be lost if information is not shared as it should be. Indeed the new Caldicott Principle recognises this when it states 'the duty to share information can be as important as the duty to protect confidentiality'.

The rules within this guide are applicable to everyone using or sharing confidential information which has been collected through publicly funded health and adult social care activities concerning or related to the provision of care for an individual. This could include, for example, the costs of their treatment as well as information within the care record.

The guide describes the confidentiality rules that people are entitled to expect to be followed in care settings run by the NHS or publicly funded adult social care services. Therefore, if a patient has an operation in an NHS hospital and is discharged to an independent care home (within the private or voluntary sector) for which public funding is received, that independent provider should also follow this guide when handling the information sent to support ongoing care.

The independent sector has been fully involved in developing this guide. All organisations are encouraged to follow the guide, which summarises existing laws, principles and obligations in an accessible way.

Whilst the guide does highlight how the rules can be applied in practice, it is not restricted to good practice so provides readers with a full picture of what they should do and why.

# What are the confidentiality rules?

## Rule 1

Confidential information about service users or patients should be treated confidentially and respectfully.

## Rule 2

Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.

## Rule 3

Information that is shared for the benefit of the community should be anonymised.

## Rule 4

An individual's right to object to the sharing of confidential information about them should be respected.

## Rule 5

Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

# Rule 1

Confidential information about service users or patients should be treated confidentially and respectfully

Underpinning the law and professional codes of practice, there are basic issues of right and wrong. It is right to respect people's privacy and wrong to betray their confidences. Prying and gossiping are recognised as unethical in all settings and in all walks of life.

## A. Maintaining trust and respect should always be a priority

The duty of confidentiality is based on trust and respect and this is fundamental to safe and effective care. An environment of trust encourages people to be open and honest with those who care for them and to provide all the details necessary so that they receive the best care possible. People need to trust that their confidential information is safe when confiding in a doctor, nurse, social worker or other professional.

In the unlikely event that confidential information about an individual is inappropriately disclosed, the individual should always receive an explanation and an apology from the individual or the organisation responsible.

## B. Professional confidentiality obligations should always be respected

Preserving privacy and confidentiality is essential for health and social care professionals. Organisations should recognise that the professionals they employ are accountable to their regulators for protecting confidentiality. This guide is consistent with regulatory advice although some regulators may impose additional obligations[6].

Organisations need to recognise professional standards and avoid imposing contradictory rules. Professionals need to maintain the trust of individuals and the public. They risk being disciplined and struck off a professional register if they fail to do so by breaching confidentiality. Organisations should ensure that equivalent organisational rules apply to non-regulated staff, such as administration and management staff, as part of their contract of employment obligations.

## C. To retain an individual's trust and to support safe care, the care record should be as complete as possible, accurate and fit for purpose

A key part of the trust relationship is ensuring that the care record (including elements such as x-rays and test results, not just paper and computerised case notes or records) is complete, accurate and fit for purpose. Information is not safe if it is not accurate. It is the responsibility of each member of the care team to ensure this. They should collect the confidential information in a way that makes it easy to share relevant information appropriately. There should be systems in place to ensure information is available when it is needed in a timely manner. Aided by good clear records, service users and patients can fully participate in decisions about their care[7].

6 Further details are available in section 5 ('Professional regulators' guidance') of the references document available at www.hscic.gov.uk/confguideorg

7 Further details are available in section 6 ('Record-keeping best practice') of the references document available at www.hscic.gov.uk/confguideorg

# Rule 2

Members of a care team should share confidential information when it is needed for the safe and effective care of an individual

It is vitally important that health and social care professionals understand that they have a duty to share confidential information in the best interests of an individual in their care – when they are providing 'direct care'[8]. Confidential information should be shared within the direct care team if that is expected to result in better or safer care. Most people who use health and social care services assume social workers, doctors, nurses and other professionals will share confidential information among the care team.

Sometimes individuals are put at risk when confidential information is not shared. For example, a vulnerable adult being looked after by a care worker who does not know what medication was prescribed when they were discharged from hospital. Tragically, lives have been put at risk when information has not been shared and this has been identified as the root cause of failure in many serious case reviews, such as the Baby P[9] case.

However, even where it is clearly beneficial to share information for direct care, rules about confidentiality and privacy still apply. That means that only those who have a clear 'need to know' should have access to the relevant confidential information.

## A. Confidential information should be shared for safe and effective care

### Sharing with whom?

Of course, the individual has a right to see their records and this should be at the forefront of the minds of those recording notes and administering care.

Safe and effective care is dependent upon relevant confidential information being shared amongst all those involved in caring for an individual. Generally, individuals should be informed about who will see their confidential information. Without such advice they may not be aware of the wide range of staff who are part of the direct care team, including social workers, doctors, nurses, laboratory staff, social care staff, those that provide specialised care and the administrative staff who support care provision. When an individual agrees to being treated by the wider care team it creates a direct care relationship between the individual and the professional, as well as their team. In these situations it is reasonable for staff to assume that the individual is also agreeing to confidential information about them being shared by the care team[10].

An individual's decision about particular pieces of information being shared or not being shared within the care team, or with others providing care, should be respected. However, there are other duties or obligations that might outweigh the duty of confidentiality, for example the obligation to report notifiable diseases[11].

An individual may decide to withdraw their consent (permission) to a disclosure of particular items of confidential information that members of staff consider to be essential to the provision of safe care. In circumstances where an individual does 'opt out' or withdraw their consent, staff should explain that failure to disclose that information may compromise the individual's care.

8 Further details are available in section 7 ('Sharing information for direct care') of the references document available at www.hscic.gov.uk/confguideorg

9 www.haringeylscb.org/executive_summary_peter_final.pdf

10 The basis of sharing within the care team is 'implied consent' and therefore without a 'legitimate relationship' being established between the individual and the member of the care team, there is no consent. Examples of circumstances where information might be shared to provide or support care are given in section 7 ('Sharing information for direct care') of the references document available at www.hscic.gov.uk/confguideorg

11 Public Health (Control of Disease) Act 1984 and amendments. See in particular the Heath Protection (Notification) Regulations 2010 (SI 2010/659)

This could include opting out of having a Summary Care Record. The Summary Care Record enables healthcare staff caring for an individual to be made aware of any current medications or allergies they may suffer from. This confidential information can ensure that safe treatment can be provided in an emergency situation. Some patients may have already communicated their wish to opt out of their clinical information being used in a Summary Care Record and this wish will continue to be respected and implemented.

Often clinicians will be aware that they are working with only parts of confidential information and should balance the risks and benefits of proceeding with care with only parts of the information. In some exceptional cases, an individual's request not to share confidential information within the care team may effectively mean that care cannot be provided. The individual's choice to refuse to share confidential information about them in this way is tantamount to refusal of care. However, individuals do have the right to choose whether or not to accept a form of care.

Individuals may also choose whether confidential information about them can be shared more widely than the direct care team, for example with family members or carers. Where the individual lacks the capacity to decide, it may be judged that sharing confidential information with a carer or family member is beneficial for their care.

When considering whether to share confidential information with a carer or family member, the guidance below should be followed[12]:

- professionals should establish with the service user or patient what information they want to be shared, with whom, and in what circumstances.
- confidential information should be shared with the carer when the service user or patient has given explicit, informed consent and when the carer consents to be told.
- where the service user or patient does not have capacity to give valid consent, confidential information should be shared with the carer where it is in the person's best interests.

## B. When confidential information is shared it should be relevant, necessary and proportionate

### What should be shared?

When confidential information is shared within the care team, only information that is relevant, necessary and proportionate should be shared. Close attention must be paid when applying this test to avoid compromising care. There are data protection principles [13] involved, such as the need to demonstrate that:

- there is a clear purpose, for example to help with a diagnosis.
- the purpose could only be achieved by the sharing of confidential information.
- the extent of the information sharing is kept as limited as possible, consistent with achieving the clear purpose.

12 Further details are available in section 8 ('Carers, family members and friends') of the references document available at www.hscic.gov.uk/confguideorg

13 Further details are available in section 3 ('The Data Protection Act 1998') of the references document available at www.hscic.gov.uk/confguideorg

Where confidential information is stored in a way that makes it practicable to separate pieces of confidential information, it is not acceptable to share all information in an individual's care record unless the confidential information is relevant and appropriate to the individual's care. For example, only part of a patient's medical history may be relevant to a new referral so the rest of the medical record should not be shared unless there is a clinical reason to do so. In circumstances where it is impossible to separate out the relevant information, such as in the case of paper records, sharing in the interests of care is the priority. Confidentiality should not become a barrier to safe and effective care.

It is important to remember that individuals have different needs and values. Even if something does not appear to be sensitive, it may be considered to be sensitive by the individual service user or patient. It is likely that individuals will regard matters relating to their mental and sexual health as particularly sensitive. There are special rules that apply to information concerning these matters[14].

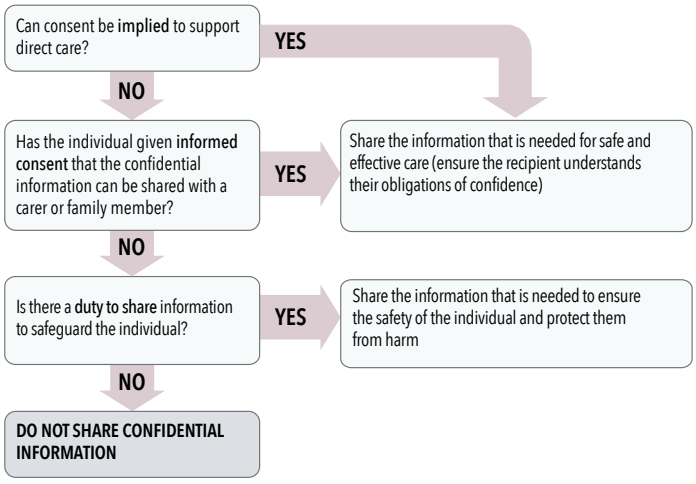
## C. However under some circumstances professionals have a **duty to share** confidential information about individuals in their care

### Safeguarding

The need to share confidential information becomes an absolute imperative in cases involving a threat to the safety of others. An example of this could be the prevention of abuse of a vulnerable elderly person. This may necessitate the sharing of confidential information with the police or other organisations.

In addition, everyone who comes into contact with families has a role to play in safeguarding children. Where there is reasonable cause to believe that a child or young person may be suffering or may be at risk of suffering significant harm, practitioners should always consider referring their concerns to children's services or the police[15].

**Fig 1. Deciding whether to share confidential information for direct care**




14 Further details are available in section 7 ('Sharing information for direct care') of the references document available at www.hscic.gov.uk/confguideorg

15 Further details are available in section 9 ('Safeguarding') of the references document available at www.hscic.gov.uk/confguideorg

# Rule 3

Information that is shared for the benefit of the community should be anonymised

Information that has been collected by health and social care services while providing direct care for individuals has the potential to provide huge benefits for the community. However, to protect the individual's confidentiality, anonymised information should be used wherever possible when it is for the benefit of the community, rather than in support of direct care[16].

Information is considered to be anonymised when there is little or no risk of an individual being identified[17]. This could include information that has been summarised and presented in a table[18] for the purposes of analysis. Information collected in support of direct care is of enormous value when assessing the quality and efficiency of health and social care services and identifying how they can be improved. Such work includes the use of anonymised information about individuals who have suffered from a particular disease or have undergone a particular treatment.

This information may also be of huge benefit to researchers trying to find new and better cures. The experiences of individuals on a particular care pathway may help commissioners to improve services for the benefit of future users. Public health specialists running health improvement programmes to increase life expectancy or reduce health inequalities may need to combine information from different sources to build up a picture of how people's health outcomes relate to their individual lifestyles and environment.

Those using information should always ensure that they minimise the risk of identifying an individual. The guiding principles about the type of information which should be used for different purposes are considered below in the order in which they should be addressed:

1. Will anonymised information be sufficient for the purpose? This sort of information can be published and used without limitations (Part A).

**IF NOT**

2. Will de-identified information (information which identifies an individual has been removed, but there is still some risk of re-identification) be sufficient for the purpose? There are two ways to protect de-identified information so it can be considered to be 'anonymised':

- Where there is a low risk of re-identification, appropriate[19] agreements or contracts can be put in place, which limit how the information can be used.
- Where there is a higher risk of re-identification, stricter controls can be put in place to create a trusted environment for the information (Part B).

**IF NOT**

Is there a lawful basis to use confidential information (Part C)?

16 A detailed explanation of the boundary between 'direct care' (the subject of rule 2) and 'indirect care' (the subject of this rule) is provided in section 10 ('Using health and social care information - direct care and indirect care purposes') of the references document available at www.hscic.gov.uk/confguideorg

17 Further guidance on anonymisation techniques is available in section 12 ('Anonymisation guidance') of the references document available at www.hscic.gov.uk/confguideorg

18 Often referred to as aggregate information, where entries that may enable individuals to be identified have been removed.

19 See section 14 ('Data sharing contracts and agreements') of the references document available at www.hscic.gov.uk/confguideorg

Rule 3

All health and social care organisations should clearly explain to patients, service users and the public how the confidential information they collect could be used in de-identified form for research, audit, public health and other purposes[20].

## A. Generally, anonymised information can and should be used to support the improvement of care services

### Effectively anonymised information can be published

Removing the individual's name, age, address and other personal identifiers[21] may not be sufficient to effectively anonymise the information. This is because it is sometimes possible to link pieces of information together which on their own would not identify an individual but when looked at together could re-identify an individual. For the same reason anonymisation is not always achieved through masking the individual's identity by using pseudonyms or coded references.

When confidential information has been anonymised in line with the HSCIC Anonymisation Standard[22] or equivalent, it can lawfully be published and used. This means it can be shared without breaching confidentiality.

## B. However, sometimes anonymised information by itself is not sufficient to release benefits to the community

Sometimes anonymised information is not adequate to support important activities. Occasionally it is important to have information at service user or patient level, which allows for a differentiation between individuals. Although the information is not identifiable, there is still a risk that an individual could be identified unless appropriate controls are put in place. The controls required will be based on the risk of re-identification of an individual.

The risk is deemed to be low where personal identifiers have been removed. This risk can be controlled by data sharing agreements or contracts with appropriate liabilities and penalties included.

### Anonymisation within a 'trusted' environment

The risk is higher where, for example, a single personal identifier is used and the controls required must be more robust. An example of this is where commissioners of integrated social care and health services for people with complex needs want to plan improved care pathways. They may need to know one identifying characteristic about the individuals concerned to ensure they are making best use of the services in the community. To achieve these benefits, information about the same person needs to be linked together by the use of one identifying characteristic, but there is no need to know who the individual is.

20 More information about fair processing and the level of transparency required can be found in section 3 ('The Data Protection Act 1998') of the references document available at www.hscic.gov.uk/confguideorg

21 Other examples of personal identifiers include (but are not restricted to) date of birth, post code, local hospital number, national insurance number and telephone number. Further guidance can be found in section 1 ('The Information Governance Review') of the references document available at www.hscic.gov.uk/confguideorg

22 www.isb.nhs.uk/library/standard/128

Such linkage may only be performed within a trusted environment which applies strict controls. When this is done the information in the possession of that organisation or person can be considered to be anonymised. It would not be anonymised if it were shared outside of those controls or published.

The controls need to be sufficient to ensure the recipient has created a 'trusted environment'[23]. Examples include:

- signed contracts or agreements which stipulate how the information will be used, including restrictions on linking information to prevent the re-identification of individuals. (See, for example, the HSCIC data sharing contract[24])

**AND**

- demonstration of meeting the required standards of security and privacy, for example the Information Governance Toolkit (IGT)[25].

**AND**

- an independent auditor's opinion of security and privacy measures.

The information ceases to be confidential information and is considered 'anonymised' only by virtue of the controls in place.

## C. In exceptional circumstances it may be necessary to use confidential information, but this requires informed consent of the individual or another legal basis which allows or mandates the sharing

Confidential information should **only** be used in those cases where it is not possible to use anonymised or de-identified information. This is only possible where:

- there is a legal obligation to share the confidential information for a particular purpose.

**OR**

- fully informed consent has been gained from the individual.

**OR**

- the law allows the sharing of confidential information for a particular purpose. This can be in the public interest or through legislation.

23 Section 13 ('Accredited Safe Havens') of the references document available at www.hscic.gov.uk/confguideorg

24 The Data Sharing Contract used by the HSCIC can be found in section 14 ('Data sharing contracts and agreements') of the references document available at www.hscic.gov.uk/confguideorg

25 www.igt.hscic.gov.uk

Each of these lawful methods is outlined below:

### Occasionally there is a legal obligation meaning that confidential information must be disclosed[26]

In some rare circumstances the law says that confidential information has to be disclosed, for example for the safety of the community. Mechanisms for this include:

- a court order, when a judge has ordered that specific and relevant information should be disclosed and to whom.
- legislation imposing a statutory duty to notify a 'Proper Officer' of a local authority if staff know of or suspect that a patient is suffering from a notifiable disease[27].
- legislation giving powers to the HSCIC to collect information from providers[28]. Although these are mandatory on providers, please see rule 4 which gives the individual the right to object to confidential information about them being shared.

### The possibility of gaining fully informed consent should be explored

Gaining an individual's consent by asking their permission should always be considered as an option for providing a lawful basis for sharing confidential information. The consent must be informed and must not be open ended. The purpose of sharing the confidential information must be made clear to the individual as it is on that basis that they provide consent. If individuals are not informed about how confidential information about them is shared it may have serious consequences including complaints, legal action and significant fines. People are entitled to have their consent and objections reliably recorded so they are available to be shared and their wishes respected.

### Where informed consent is not feasible, a legal basis allowing the sharing of confidential information should be explored

There are a few limited examples where the individual's right of confidentiality may be overruled for the 'public interest'. These are generally cases relating to a single individual's information and the public interest will almost never provide the basis for routine sharing arrangements. Confidential information can be disclosed to support the detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others.

Decisions to disclose confidential information when legal permission is available are complex. The holder of the information must believe that the public good that would be served by sharing the information outweighs both the obligation of confidentiality owed to the individual and the public good of protecting trust in a confidential service.

26 Further details of legal obligations to disclose confidential information are available in section 16 ('Legislation that controls confidential information disclosures') of the references document available at www.hscic.gov.uk/confguideorg

27 Public Health (Control of Disease) Act 1984 and amendments. See in particular the Heath Protection (Notification) Regulations 2010 (SI 2010/659)

28 The Health and Social Care Act 2012. Full details are available in section 15 ('The Health and Social Care Information Centre's powers under the Health and Social Care Act 2012') of the references document available at www.hscic.gov.uk/confguideorg

There are also regulations and legislation[29] which allow for the sharing of confidential information. For example, when applying for 'section 251 support' [30] a high threshold (but lower than the public interest test) must be met before the duty of confidentiality can be set aside for the purposes of research, audit and other medical purposes that are not directly associated with care[31].

## D. For all of the lawful methods of sharing confidential information above, **all** of the following three conditions should be met[32]:

### 1. Individuals should be informed about how their confidential information may be shared or used

The law[33] says that any organisation holding confidential information should ensure there are no surprises for individuals about how it is used. There are some exceptions, for example where it would compromise a criminal investigation or where information is shared for safeguarding reasons.

As a minimum, individuals should be told:

- what confidential information is held about them.
- who may access it and/or who it may be provided to.
- the purpose it is being used for.
- how they can raise an objection.

Where confidential information passes through several organisations which are not directly involved in an individual's care, it can become increasingly difficult to meet this requirement. Even where it is not pragmatic for an individual to be informed directly, each body in the chain must publish the information above in a prominent and accessible form (for example on a website).

### 2. Steps should be taken to use the minimum level of confidential information necessary to support the purpose

In all cases the minimum level of confidential information necessary to achieve the purpose should be used[34].

29 Such as the Crime and Disorder Act 1998 section 115, the Data Protection Act 1998 section 29, and the Police and Criminal Evidence Act 1984

30 Section 251 of the NHS Act 2006 (commonly referred to as 'section 251'). The Health Service Control of Patient Information Regulations 2002 invoked are the regulations which allow the Secretary of State to exercise judgement as to whether the duty of confidentiality should be set aside

31 Further details can be found in section 16 ('Legislation that controls confidential information disclosures') of the references document available at www.hscic.gov.uk/confguideorg

32 Because confidential information is also personal, the Data Protection Act 1998 still applies. The principles within it are outlined here in respect of confidential information. These conditions also apply to the use of confidential information for direct care and are covered in rule 2

33 The Data Protect Act 1998. More information about fair processing and the level of transparency required can be found in section 3 ('The Data Protection Act 1998') of the references document available at www.hscic.gov.uk/confguideorg

34 Where explicit consent has been obtained, the amount of confidential information shared should be determined in relation to the terms of consent

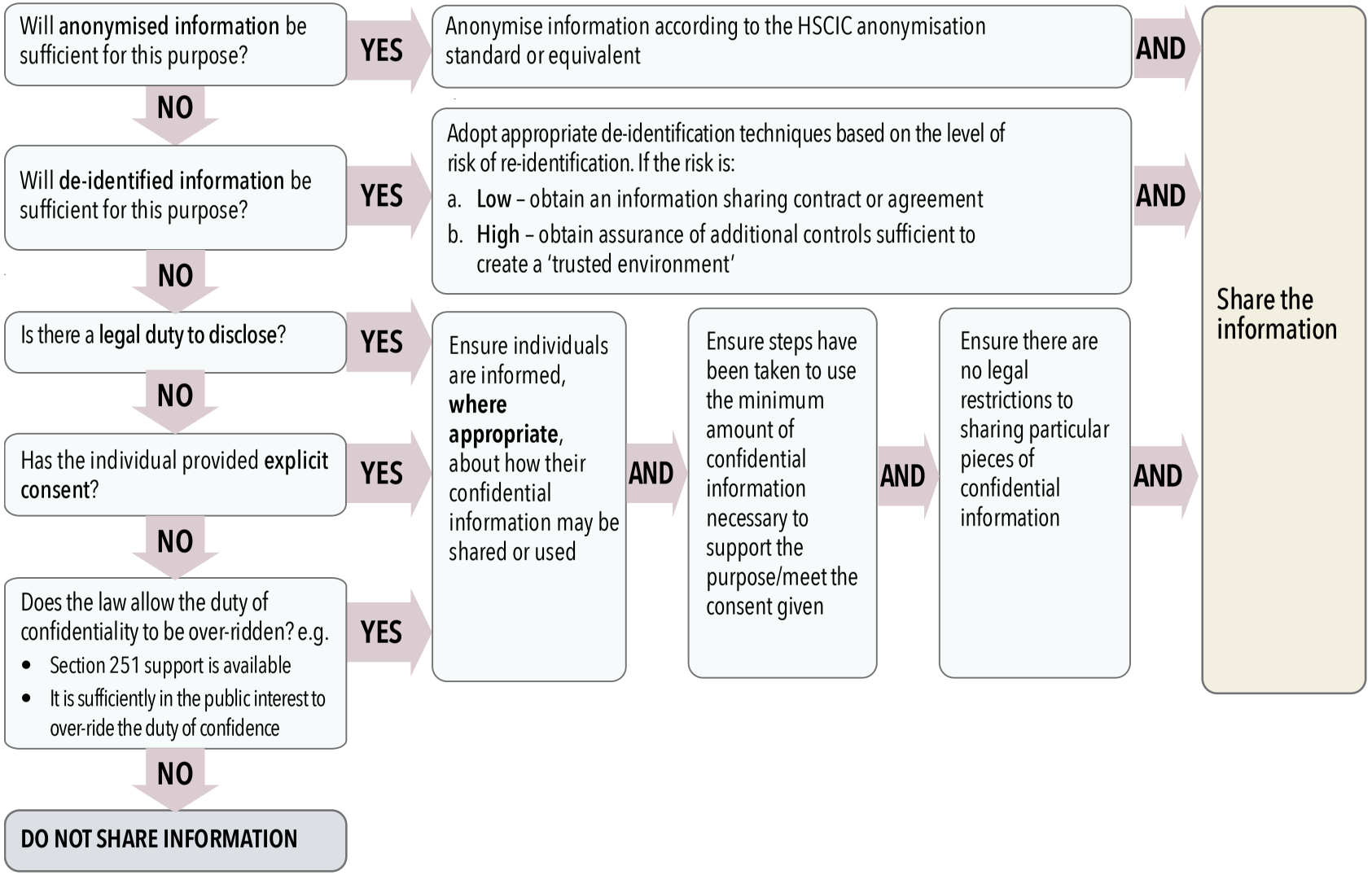
### 3. The law should be checked to ensure there are no legal restrictions to sharing particular pieces of confidential information

Information should always be shared in accordance with the law and organisations must abide by legal provisions which ban or limit the sharing of particular pieces of confidential information[35]. One example is the law which makes the disclosure of information relating to assisted conception treatment (for example information about gamete donors and people receiving treatment) a criminal offence in most cases[36].

35 Further details can be found in section 16 ('Legislation that controls confidential information disclosures') of the references document available at www.hscic.gov.uk/confguideorg

36 Section 33A and section 41 of the Human Fertilisation and Embryology Act 1990

## Fig 2. Deciding whether to share or disclose confidential information for the benefit of the community




Rule 3

# Rule 4

An individual's right to object to the sharing of confidential information about them should be respected

Individuals have a right to object to confidential information about them being used or shared beyond their treatment and care and to have that right respected.

Rule 2 addresses how to respect the choices of individuals in relation to the sharing of confidential information about them for direct care purposes.

The general principles governing how health and social care organisations should handle objections are explained below in part A. Specific rules governing the sharing of confidential information from GP records for indirect care are set out in part B. The sharing of anonymised information in circumstances where an objection to the sharing of confidential information is implemented is explained in part C. Circumstances when individuals' objections may or must be overruled are set out in part D.

## A. In all cases, objections should be considered consistently and individuals should receive an explanation of the likely consequences of their decisions

Organisations should ensure that members of staff show respect for the wishes of any individual who objects to particular items of confidential information being shared. The likely consequences of an objection should be explained to the individual to aid an informed decision.

To ensure objections are considered consistently, organisations should review the criteria for assessing objections on an ongoing basis.

## B. When individuals object to the sharing of confidential information from GP practices for indirect care, confidential information will not be shared

Parts of patients' records will be sent by GP practices to those who have special approval to use health information for purposes other than direct care. A specific example will be where GP practices send parts of patients' records to the HSCIC where the information will be anonymised and used to benefit the community. Any patient may object to confidential information about them being sent from a GP practice or being shared onwards by the HSCIC. In either case, the patient's objection should be implemented. This means that if a patient tells their GP that they:

- do not want information about them leaving a GP practice in identifiable form for purposes other than direct care, then confidential information about them will not be shared. AND/OR
- do not want information about them leaving the HSCIC in identifiable form, then confidential information about them will not be sent to anyone by the HSCIC.

### C. Where an objection to the sharing of confidential information is implemented, anonymised information can be shared

Sharing anonymised information where an individual objects to the sharing of confidential information about them means that the individual's confidentiality wishes are respected.

Anonymised information about service users and patients contributes towards the improvement of services that they and the community benefit from, without infringing their privacy or disrespecting their confidentiality wishes.

### D. In rare cases where the likely consequences of an objection pose such a significant risk that the objection is lawfully overruled, individuals should receive an explanation

There are rare circumstances when part of an individual's objection (relating to a particular piece of information) may, or must, be overruled by law. Individuals should be made aware of these when they object. It should be made clear whether the law requires that their objection 'must' be overruled, or 'may' be overruled.

When the law says there is an obligation to share the confidential information, for example in the case of notifiable diseases[37], the individual should receive an explanation of why their objection must lawfully be overruled.

When the law allows pieces of confidential information to be shared, for example where there is an overwhelming public interest justification, the individual should receive an explanation of why the available permission has or has not been used in their case. The exception is where it is judged that informing an individual might prejudice the purpose of sharing (e.g. where serious crime is suspected) or might put someone at risk[38].

37 Public Health (Control of Disease) Act 1984 and amendments. See in particular the Heath Protection (Notification) Regulations 2010 (SI 2010/659)

38 The rules surrounding objections are complex and further guidance can be found in section 18 ('Objections to sharing') of the references document available at www.hscic.gov.uk/confguideorg
Please also note the fair processing requirements and details of the level of transparency required, which can be found in section 3 ('The Data Protection Act 1998') of the references document available at www.hscic.gov.uk/confguideorg

# Rule 5

Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed

Rule 5

Organisations should ensure that they have the appropriate organisational and technical systems security, policies, processes and staff training and education to ensure that confidential information is held and shared securely[39] and appropriately, as set out in this guide. Every organisation should:

### A. Appoint a senior individual responsible for ensuring the confidentiality rules are followed

An identified senior individual within each health and social care organisation should be appointed as being responsible for ensuring the organisation continues to meet its requirements as set out in this guide. This individual will be responsible for ensuring the organisation complies with the law in relation to confidentiality. This should be the Caldicott Guardian[40] or other senior member of staff responsible for information risk. The guide will be an evolving document and organisations should review their compliance and update their policies and procedures in line with any changes to the guide, at least annually.

### B. Complete an Information Governance Toolkit Assessment (IGT)

The IGT defines and draws together many of the information governance requirements that apply in different circumstances. One way to demonstrate that appropriate policies, procedures and systems are in place is for organisations to comply with relevant IGT requirements[41]. Examples of key requirements include:

- access should be limited to those authorised, with a need to know.
- confidential information should be held and distributed securely.
- some confidential information should not be retained indefinitely and should be securely disposed of at the appropriate time[42].
- staff should be trained and educated appropriately to discharge relevant duties.

### C. Ensure that all organisations with which it shares confidential information are committed to following the confidentiality rules

There is an important obligation on the organisation sharing the confidential information to ensure that recipients can demonstrate that they can be trusted to handle it in accordance with the confidentiality rules.

39 Details can be found in section 17 ('Information security management') of the references document available at www.hscic.gov.uk/confguideorg

40 A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing. The guardian plays a key role in ensuring that the NHS, councils with social services responsibilities and partner organisations satisfy the highest practicable standards for handling patient identifiable information

41 The full set of IGT requirements are available at www.igt.hscic.gov.uk

42 Guidance on retention and secure disposal of confidential information can be found in section 6 ('Record-keeping best practice') of the references document available at www.hscic.gov.uk/confguideorg

For high volumes and high sensitivity information, an appropriate information sharing agreement or contract is required to provide clarity on expected practice and any specific restrictions e.g. prohibition of onward sharing of information without permission[43].

A Privacy Impact Assessment (PIA) is an invaluable tool when assessing the impact on an individual's privacy of using the information and what control measures are necessary and proportionate whilst placing the privacy of individuals at the forefront of all decisions[44].

For organisations outside health and social care (for example the police), some of the specific organisational controls in rule 5 will not apply, but it is expected that their own organisational confidentiality and privacy controls will provide equivalent assurance.

## D. Encourage people to report concerns that the confidentiality rules have not been followed

Organisations should have processes in place to encourage people to report concerns that the confidentiality rules are not being followed. If they feel their concerns about confidentiality and safe and effective sharing of information have not been appropriately dealt with by the organisation they should have easy access to the organisation's whistle-blowing procedure.

Staff need to know that they can safely share confidential information with a particular body. Therefore, they must be informed of serious concerns so they know when they should assess the risk and perhaps not share confidential information with a particular organisation.

43 The Data Sharing Contract used by the HSCIC can be found in section 14 ('Data sharing contracts and agreements') of the references document available at www.hscic.gov.uk/confguideorg

44 Guidance on how to conduct a PIA is available in section 11 ('Privacy Impact Assessments') of the references document available at www.hscic.gov.uk/confguideorg

# Appendix 1

## The Information Governance Review - To Share or Not to Share?

### The Caldicott principles

1. **Justify the purpose(s)**
   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. **Use the minimum necessary personal confidential data**
   Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.
4. **Access to personal confidential data should be on a strict need-to-know basis**
   Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
5. **Everyone with access to personal confidential data should be aware of their responsibilities**
   Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. **Comply with the law**
   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
7. **The duty to share information can be as important as the duty to protect patient confidentiality**
   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

# Notes

hscic Health & Social Care Information Centre

# A guide to confidentiality in health and social care

## Treating confidential information with respect

Published by the
Health and Social Care
Information Centre

**www.hscic.gov.uk**
**0845 300 6016**
**enquiries@hscic.gov.uk**