

CONSENT GUIDANCE FOR INFORMATION SHARING

1. Introduction

The aim of this document is to give guidance to enable personal information concerning service users to be shared between organisations without compromising confidentiality unless there is a legal requirement, or an overriding public interest to do so.

Confidentiality is an essential requirement for the preservation of trust between service users and health professionals and is subject to legal and ethical safeguards. Service users should be able to expect that information about their health which they give in confidence will be kept confidential unless there is a compelling reason why it should not. There is also a strong public interest in maintaining confidentiality so that individuals will be encouraged to seek appropriate treatment and share information relevant to it.

As a general principle all personal information must only be collected, held and shared on a strict 'need to know' basis and all decisions to share information that are not directly associated with the direct continuing healthcare of the patient should be recorded.

2. Purpose

The purpose of this document is to provide specific guidance for all staff on consent and information sharing issues. This document forms an appendix to the Trust's Information Sharing & Consent Policy and Procedure.

3. Consent

Consent is required in all cases of sharing service user identifiable information unless disclosure is required by law, or there is an overriding public interest in disclosure.

3.1 Definition of Consent

Consent to disclosure may be explicit or implied. It may also be consent to disclosure of specific information to a particular person or body for a particular purpose or it may be consent to general future disclosure for particular purposes. In either case consent should be informed and freely given.

Consent is defined in "Confidentiality: NHS Code of Practice (2003) as follows:

(a) Informed Consent

All consent should be fully informed. Every patient should be informed about what happens to the information they give to the NHS (it is the minimum requirement under the General Data Protection Regulation). For each episode of care you should ensure that your service user is aware of who will see their information and what you will be doing with it and give them the

CPG60 - INFORMATION SHARING & CONSENT PROCEDURE

opportunity of saying 'no' to information sharing, unless legislation dictates otherwise.

All service users should receive the following information:

- Who the Data Controller is
- Why the information is needed
- The purposes for which the information will be processed
- Who will see the information
- Any disclosures that may need to be made to other organisations (e.g. Acute Hospitals, Social care, Clinical audit, GP, Mental Health Teams, Drug Teams etc)
- The circumstances in which information may be disclosed without consent, where there is an overriding public interest (e.g. child protection, or serious crime.)
- Information restricted by legislation (e.g. serious communicable diseases.)
- Information that must be passed on because of legislation (e.g. births, deaths, cancer registries, abortion.)

If service users have any reservations about information sharing then explain that the direct continuing care could be affected by restrictions placed on sharing. If service users still refuse to share any information then you have not gained consent for that particular information and the service user's wishes must be respected (unless there is a legal requirement, or an overriding public interest in disclosure.)

(b) **Implied Consent**

Service user agreement that has been signalled by behaviour (this consent also needs to be fully informed).

Implied consent is not a lesser form of consent but in order for it to be valid it is important that service users are made aware that information about them will be shared, with whom it will be shared, and of their right to refuse. Health professionals bear responsibility for the disclosures they make, so when consent is taken to be implied, they must be able to demonstrate that the assumption of consent was made in good faith and based on good information. If not, it is no consent at all and some other justification will be needed for its disclosure. In addition to information provided face to face in the course of a consultation, leaflets, posters and information included with an appointment letter can play a part in conveying to service users the reality and necessity of information sharing. Implied consent is usually sufficient for direct service user care (see paragraph 4.1 below).

(c) **Express/Explicit Consent**

Articulated service user agreement. Clear and voluntary indication of preference or choice, usually given orally or in

writing and freely given in circumstances where the available options and the consequences have been made clear. Explicit consent is the ideal as there is no doubt as to what has been agreed.

3.2 Recording Consent

Record in the service user's record if the service user has been provided with and understands the notice/leaflet regarding information sharing and has not said 'no' to sharing any part of their information.

Where a service user has refused to share information this should be recorded in the service user's record, dated and time stamped. That information must not be shared (unless there is a legal requirement or an overriding public interest in disclosure.)

3.3 Keeping Consent Up To Date

It is essential that children, once they gain capacity, are asked to confirm their own choice, as a previous recorded choice regarding consent will have been made by another party, on their behalf, which may not reflect their own choice.

It may also be essential to revisit the consent at other times e.g. when changes which impact on how information is used are introduced. Consent should also be reviewed whenever there are changes to information sharing/disclosure during an episode of care.

4. What You Need To Know Before Sharing Information

4.1 Sharing Information With Other Health Professionals

In the absence of evidence to the contrary, service users are normally considered to have given implied consent for the use of their information by health professionals for the purpose of the care they receive. Information sharing in this context is acceptable to the extent that health professionals share what is necessary and relevant for service user care on a 'need to know' basis. Healthcare and social care although often closely related, do not always fall into the same category, and disclosures of information to social care usually require explicit consent from competent service users. Sometimes two competing interests come into conflict, such as the service user's informed refusal to allow disclosure, and the need to provide effective treatment to that person. A service user's refusal to allow information sharing with another health professional may compromise service user safety, but if this is an informed decision by a competent person it should be respected.

4.2 Multi – Agency Working

Health professionals during the course of their treatment of service users will have contact with partner organisations from time to time. These include social care, housing and benefits agencies. Health professionals should from the outset discuss with service users the desirability of sharing information with other agencies as appropriate.

Other agencies may wish to be involved in discussions about service users at various points in their treatment, or to attend case conferences, or multi-disciplinary meetings. Health professionals may also be invited to attend external case conferences organised by partner organisations to discuss the health and welfare of service users. In all these circumstances information sharing should take place with explicit consent or in the absence of explicit consent where disclosure is required by law, or there is an overriding public interest in disclosure.

4.3 Assessment Of Capacity

All people aged 16 and over are presumed, in law, to have the capacity to give or withhold their consent to disclosure of confidential information unless there is evidence to the contrary. A service user who is suffering from a mental disorder or impairment does not necessarily lack the capacity to give or withhold their consent. Equally, service users who would otherwise be competent may be temporarily incapable of giving valid consent due to factors such as extreme fatigue, drunkenness, shock, fear, severe pain or sedation. The fact that an individual has made a decision that appears to others to be irrational or unjustified should not be taken on its own as conclusive evidence that the individual lacks the mental capacity to make that decision. If, however, the decision is clearly contrary to previously expressed wishes, or is based on a misperception of reality, this may be indicative of a lack of capacity and further investigation will be required.

There is no presumption of capacity for people under 16 in England, and Wales, and those under this age must demonstrate their competence by meeting certain standards set by the courts. The central test is whether the young person has sufficient understanding and intelligence to understand fully what is proposed.

To demonstrate capacity individuals should be able to:

- Understand in simple language (with the use of communication aids, if appropriate) what is to be disclosed and why it is being disclosed
- Understand the main benefits of disclosure
- Understand, in broad terms, the consequences of disclosure
- Retain the information long enough to use it and weigh it in the balance in order to arrive at a decision
- Communicate the decision (by any means)
- Make a free decision (i.e. free from undue pressure)

4.4 Adults Who Lack Capacity

4.4.1 Temporary Or Permanent Mental Incapacity

Service users with mental disorders or learning disabilities should not automatically be regarded as lacking the capacity to give or withhold their consent to disclosure of confidential

information. Unless unconscious, most people suffering from a mental impairment can make valid decisions about some matters that affect them. An individual's mental capacity must be judged in relation to that particular decision being made. If therefore a service user has the requisite capacity, disclosure of information to relatives or third parties requires service user consent. One of the most difficult dilemmas for health professionals occurs where the extent of such service user's mental capacity is in doubt. In such cases health professionals must assess the information which is available from the service user's health record and from third parties. They should attempt to discuss with service users their needs and preferences as well as assess their ability to understand their condition and prognosis. If there is still doubt about a service user's competence to give or withhold consent, health professionals should seek a second opinion.

4.4.2 Relatives, Carers And Friends

If a service user lacks capacity, health professionals may need to share information with relatives, friends or carers to enable them to assess the service user's best interests. Where a service user is seriously ill and lacks capacity, it would be unreasonable always to refuse to provide any information to those close to the service user on the basis that the service user has not given explicit consent. This does not, however, mean that all information should be routinely shared, and where the information is sensitive, a judgement will be needed about how much information the service user is likely to want to be shared, and with whom. Where there is evidence that the service user did not want information shared, this must be respected.

4.4.3 Next Of Kin

Although widely used, the phrase 'next of kin' has no legal definition or status. If a person is nominated by a service user as next of kin and given authority to discuss the service user's condition, such a person may provide valuable information about the service user's wishes to staff caring for the service user. However, the nominated person cannot give or withhold consent to the sharing of information about the service user and has no rights of access to the service user's medical records. The service user may nominate anyone as next of kin. In the absence of such a nomination, no-one can claim to be next of kin.

4.4.4 Proxy Decision-Makers

In England and Wales, the Mental Capacity Act 2005 allows people over 18 years of age who have capacity to appoint a welfare attorney to make health and personal welfare decisions once capacity is lost. The Court of Protection may also appoint a deputy to make these decisions. Where a service user lacks

capacity and has no relatives or friends to be consulted, the Mental Capacity Act requires and Independent Mental Capacity Advocate to be appointed and consulted about all decisions about 'serious medical treatment', or place of residence. An attorney or deputy can also be appointed to make decisions relating to the management of property and financial affairs. In the case of health information, health professionals may only disclose information on the basis of the service user's best interests.

4.4.5 Abuse And Neglect

Where health professionals have concerns about a service user lacking capacity that may be at risk of abuse or neglect, it is essential that these concerns are acted upon and information is given promptly to an appropriate person or statutory body, in order to prevent further harm. Where there is any doubt as to whether disclosure is considered to be in the service user's best interests, it is recommended that the health professional discusses the matter on an anonymised basis with a senior colleague, the Caldicott Guardian, Information Governance Manager or Trust Solicitor. Health professionals must ensure that their concerns and the actions they have taken or intend to take, including any discussion with the service user, colleagues or professionals in other agencies, are clearly recorded in the service user's medical records

4.5 Children And Young People

4.5.1 Competent Children

There is no presumption of capacity for people under 16 in England, Wales and Northern Ireland and those under that age must demonstrate they have sufficient understanding of what is proposed. However, children who are aged 12 or over are generally expected to have capacity to give or withhold their consent to the release of information. Younger children may also have sufficient capacity. When assessing a child's capacity it is important to explain the issues in a way that is suitable for their age. If the child is competent to understand what is involved in the proposed treatment, the health professional should, unless there are convincing reasons to the contrary, for instance abuse is suspected; respect the child's wishes if they do not want parents or guardians to know. However, every reasonable effort must be made to persuade the child to involve parents or guardians particularly for important or life-changing decisions.

4.5.2 Children Who Lack Capacity

The duty of confidentiality owed to a child who lacks capacity is the same as that owed to any other person. Occasionally, young people seek medical treatment, for example, contraception, but are judged to lack the capacity to give

consent. An explicit request by a child that information should not be disclosed to parents or guardians, or indeed to any third party, must be respected except in the most exceptional circumstances, for example, where it puts the child at risk of significant harm, in which case disclosure may take place in the 'public interest' without consent. Therefore, even where the health professional considers a child to be too immature to consent to the treatment requested, confidentiality should still be respected concerning the consultation, unless there are very convincing reasons to the contrary. Where a health professional decides to disclose information to a third party against a child's wishes, the child should generally be told before the information is disclosed. The discussion with the child and the reasons for disclosure should also be documented in the child's record.

4.5.3 Parental Responsibility

Anyone with parental responsibility can give or withhold consent to the release of information where the child lacks capacity. Not all parents have parental responsibility.

- In relation to children born after 1 December 2003, both of a child's biological parents have parental responsibility if they are registered on a child's birth certificate.
- In relation to children born before these dates, a child's biological father will only automatically acquire parental responsibility if the parents were married at the time of the child's birth or some time thereafter. If the parents have never been married, only the mother automatically has parental responsibility, but the father may acquire that status by order or agreement. Neither parent loses parental responsibility on divorce.
- Where the child has been formally adopted, the adoptive parents are the child's legal parents and automatically acquire parental responsibility.
- Where the child has been born as a result of assisted reproduction, there are rules under the Human Fertilisation and Embryology Act 2008 that determine the child's legal parentage.
- In some circumstances people other than parents acquire parental responsibility, for example by the appointment of a guardian or on the order of a court.
- A local authority acquires parental responsibility (shared with the parents) while the child is the subject of a care or supervision order.
- In some circumstances parental responsibility can be delegated to other carers such as grandparents and child-minders.

If there is doubt about whether the person giving or withholding consent has parental responsibility, legal advice should be sought.

Where an individual who has parental responsibility refuses to share relevant information with other health professionals or agencies and the health professional considers that it is not in the best interest of the child (for example, it puts the child at risk of significant harm), disclosure may take place in the public interest without consent.

4.5.4 Safeguarding Children

Where health professionals have concerns about a child who may be at risk of abuse or neglect, it is essential that these concerns are acted upon and information is given promptly to an appropriate person or statutory body, in order to prevent further harm. The best interests of the child or children involved must guide decision-making at all times. Knowing what to do when service users do not want confidential information disclosed, despite this being the best way to ensure that they do not suffer harm or abuse, is very difficult for health professionals. Health professionals should not make promises to the child about confidentiality that they may not be able to keep but, as in the case of any service user, trust is best maintained if disclosure is not made without prior discussion between the health professional and the child, unless to do so would expose the child or others to an increased risk of serious harm.

Where there is any doubt as to whether disclosure is in the child's best interests, it is recommended that the health professional discusses the matter anonymously with an experienced colleague, Safeguarding Children and Families Team, the Caldicott Guardian, Information Governance Manager, Trust Solicitor, their professional body or defence body.

Health professionals must ensure that their concerns, and the actions they have taken, or intend to take, including any discussion with the child, colleagues or professionals in other agencies, are clearly recorded in the child's medical record. Health professionals may be involved in case reviews for which the child's records may need to be disclosed, but care should be taken not to disclose the notes of other family members without consent unless it can be justified in the public interest.

4.6 Best Interests

All decisions taken on behalf of someone who lacks capacity must be taken in their best interest. A best interest judgement is not an attempt to determine what the service user would have wanted. It is as objective a test as possible of what would be in the service user's

actual best interests, taking into account all relevant factors. A number of factors should be addressed including:

- The service user's own wishes (where these can be ascertained)
- Where there is more than one option, which option is least restrictive of the service user's future choices
- The view of the parents, if the service user is a child
- The views of people close to the service user, especially close relatives, partners, carers, welfare attorneys, court-appointed deputies or guardians, about what the service user is likely to see as beneficial

4.7 Public Interest

4.7.1 General Principles

In the absence of service user consent (a legal obligation or anonymisation), any decision as to whether identifiable information is to be shared with third parties must be made on a case by case basis and must be justifiable in the 'public interest'. Public interest is the general welfare and rights of the public that are to be recognised, protected and advanced. Disclosures in the public interest based on the common law are made where disclosure is essential to prevent a serious and imminent threat to public health, national security, the life of the individual or a third party or to prevent or detect serious crime. Ultimately, the public interest can only be determined by the courts. However, when considering disclosing information to protect the public interest, health professionals must:

- Consider how the benefits of making the disclosure balance against the harms associated with breaching the service user's confidentiality both to the individual clinical relationship and to maintaining public trust in a confidential service.
- Assess the urgency of the need for disclosure.
- Persuade the service user to disclose voluntarily.
- Inform the service user before making the disclosure and seek his or her consent, unless to do so would increase the risk of harm or inhibit effective investigation.
- Disclose the information promptly to the appropriate body.
- Reveal only the minimum information necessary to achieve the objective.
- Seek assurance that the information will be used only for the purpose for which it is disclosed.
- Document the steps taken to seek or obtain consent, and the reasons for disclosing the information without consent.
- Be able to justify the decision.
- Document both the extent of and grounds for the disclosure.

Health professionals should be aware that they risk criticism, and even legal liability, if they fail to take action to avoid serious harm. There is no specific legislation which tells health professionals whether or not to disclose information in a particular case, but general guidance about the categories of cases in which decisions to disclose may be justifiable are below. Guidance should be sought from the Caldicott Guardian, Information Governance Manager, Trust Solicitor, professional body or defence body where there is any doubt as to whether disclosure should take place in the public interest.

4.7.2 Serious Crime And National Security

There is no legal definition as to what constitutes a 'serious crime'. In the Police and Criminal Evidence Act 1984 a 'serious arrest-able offence' is an offence that has caused or may cause:

- Serious harm to the security of the state or to public order.
- Serious interference with the administration of justice or with the investigation of an offence.
- Death.
- Serious injury.
- Substantial financial gain or serious loss.

This includes crimes such as murder, manslaughter, rape, treason, kidnapping and abuse of children or other vulnerable people. Serious harm to the security of the state or to public order and serious fraud will also fall into this category. In contrast, theft, minor fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

4.7.3 Public Safety

A common example of what can be categorised as public safety occurs in connection with the assessment of service users with, for example, diabetes, epilepsy, defective eyesight, hypoglycaemia or serious cardiac conditions who have been advised by health professionals to discontinue driving, but who nevertheless continue. The DVLA should be informed if anybody is thought to be at risk.

Issues of public safety may similarly arise in circumstances where an individual who legitimately possesses firearms is thought by health professionals to be a risk because of drug or alcohol addiction or a medical condition such as depression. The police should be informed if anybody is thought to be at risk.

5. Information Sharing That Requires Express Consent

National guidance has identified certain areas of information sharing that must only be carried out on an express/explicit consent basis. Consent is required for information sharing that does not directly contribute to direct continuing healthcare, unless there is a robust public interest in releasing information

CPG60 - INFORMATION SHARING & CONSENT PROCEDURE

without the service user's consent or you have the express/explicit consent in writing, from the service user or recorded in the service users health record.

For most information sharing issues that are not for the direct continuing care of a service user you should consult the Caldicott Guardian or Information Governance Manager.

The following table gives further details

| | |
|--|--|
| Carers and Relatives | Generally where a service user has the capacity to consent express/explicit consent is required before sharing health information. Confidentiality can be a highly controversial issue. Carers want and need information about the person they are caring for, whereas professionals feel bound by codes of conduct on confidentiality. |
| NHS Complaints Committees | Complaint Committees will invariably need service user information. However, express consent of the complainant, and any other service users whose record may need to be reviewed, is required prior to disclosure. |
| Management Purposes | Commissioners, prescribing advisors, financial audit, resource allocation etc., - no restrictions are imposed if the data is anonymised or pseudonymised. |
| Occupational Health Professionals | Information on staff referred to occupational health departments. However, if clinicians are the service users, the powers of professional regulatory bodies for disclosure may apply. |
| Researchers | <p>The use of service user information for research goes beyond health care provision in the NHS and explicit service user consent is therefore required.</p> <p>For example, whilst most people would be happy to be included in research there may be some that might object on the grounds of, for example, 'religion'.</p> <p>However, if the research project is to use anonymised or pseudonymised data, (which is preferable) no restrictions are imposed, (refer to anonymisation and pseudonymisation below. Alternatively, an application can be made to the Ethics and Confidentiality Committee of the National Information Governance Board under section 251 of the NHS Act 2006.</p> <p>Before any research project can be undertaken an application must be made to the Local Research Ethics Committee for approval and before making any application to the Ethics and Confidentiality Committee Of the National Information Governance Board under Section 251 of the NHS Act 2006.</p> |

CPG60 - INFORMATION SHARING & CONSENT PROCEDURE

| | |
|-------------------------|--|
| Teaching | According to the Confidentiality: NHS Code of Practice teaching is not to be regarded as direct healthcare purposes and will require explicit consent. |
| Sure Start Teams | Disclosures to Sure Start teams for anything other than the direct continuing healthcare of young children needs explicit consent from parents. Example: extracting lists of children's names who are below the age of 5 from information held by an organisation to enable Sure Start to target certain groups of families to give them toothpaste samples would require explicit consent. |
| The Media | You need explicit consent to release information to the media about care and treatment (including a service user's presence in a hospital) unless there is an exceptional robust public interest in releasing information. |
| Police | Information required by the Police either needs explicit consent of the service user, a Court Order or, where criminal activities are concerned refer to section 6.1 below on Enabling Information Sharing in the Public Interest. |
| Solicitors | Solicitors requesting information must produce an up to date written signed consent from the service user before you release any information. If you have any doubts as to the authenticity of the consent or the fact that the whole of the service user's record has been requested contact the service user direct – you must obtain consent from any third parties before releasing third party information. |

6. Legislation Enabling/Requiring/Restricting Information Sharing

6.1 Enabling Information Sharing in the Public Interest

The following legislation permits information to be shared without seeking consent e.g. if you believe someone has committed serious harm, or a serious crime, However the legislation does not require you to do so. Decisions to share should be made on a case by case basis, and in the public interest.

In some circumstances, the DPA 2018 provides an exemption from particular GDPR provisions. If an exemption applies, you may not have to comply with all the usual rights and obligations.

There are several different exemptions; these are detailed in Schedules 2-4 of the DPA 2018. They add to and complement a number of exceptions already built in to certain GDPR provisions.

The exemptions in the DPA 2018 Schedules 2-4 can relieve you of some of your obligations for things such as:

1. Child Protection (Children's Act 1989 and the Protection of Children Act 1999). Allows information to be shared if a child is considered at risk of significant harm.
2. Prevention and Detection of Crime (Section 115 of the Crime and Disorder Act 1998) – e.g. request from the Police where someone is suspected of committing a serious crime.

3. Disclosures to a health professional within a Sure Start team under the NHS Act 1997 where disclosures directly and only support healthcare of young children. (If health records are to be held within partner organisations, parents must be properly informed).

Some exemptions apply to only one of the above, but others can exempt you from several things.

Some things are not exemptions. This is simply because they are not covered by the GDPR. Here are some examples:

- **Law enforcement** – the processing of personal data by competent authorities for law enforcement purposes is outside the GDPR's scope (e.g. the Police investigating a crime). Instead, this type of processing is subject to the rules in Part 3 of the Data Protection Act 2018.
- **National security** – personal data processed for the purposes of safeguarding national security or defence is outside the GDPR's scope. However, it is covered by Part 2, Chapter 3 of the DPA 2018 (the 'applied GDPR'), which contains an exemption for national security and defence.

6.2 Requiring Information Sharing

Information can be shared without consent if requested to do so by the following public bodies/officials but service users should be informed that disclosure has been required:

1. Courts, including a coroner's court, tribunals and enquiries – Only give the information requested in the order and no more. Many different Acts give courts the powers to issue court orders.
2. General Medical Council (GMC) – Entitled to access confidential patient health records as part of an investigation under the Medical Act 1983. The GMC have indicated that they would always try to obtain consent first.
3. Audit Commission – Entitled to access confidential patient health records as part of an investigation under section 6 of the Audit Commission Act 1998.
4. Health Service Ombudsman – Has the same powers as the courts to disclose person identifiable information. Any request made should be complied with, without obtaining a court order.
5. Healthcare Commission – The Healthcare Commission's legal name is the Commission for Healthcare Audit and Inspection. It was formed by the Health and Social Care Act 2003 launched on 1st April 2004.
6. Public Health and Infectious Diseases – Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1988.
7. Immunisations and vaccinations – Under the Education Act 1944 information must be passed to NHS Trusts from schools.

8. Births and Deaths – The Births and Deaths Act 1984 provides for the registration of births, still-births and deaths.
9. Abortion Regulations 1991 – a doctor carrying out a termination of pregnancy must notify the Chief Medical Officer, giving a reference number and the date of birth and postcode of the woman concerned.
10. Section 251 of the NHS Act 2006 – gives the Secretary of State for Health power to make regulations permitting the disclosure of identifiable information without consent in certain circumstances. Health professionals can apply to the Ethics and Confidentiality Committee of the National Information Governance Board, an independent public body which advises the Secretary of State for Health in England and Wales about the lawful disclosure of service user identifiable information.
11. Members of Parliament – Non-statutory investigations (e.g. Members of Parliament). If a MP states, in writing that he/she has a service user's consent for disclosure this may be accepted without further contact with the service user but – carefully consider the request and contact the service user if in any doubt.

6.3 Restricting Information Sharing

Health professionals are required by law to restrict the disclosure of some specific types of information, for example:-

1. Human Fertilisation and Embryology Act 2008
2. NHS (Venereal Diseases Regulations) 1974 and the NHS Trusts and PCTs (Sexually Transmitted Diseases) Directions 1992
3. The Gender Recognition Act 2004
4. The Adoption Act 1976

7. Anonymisation and Pseudonymisation

7.1 Anonymisation

Information can be used without service user consent and requires the removal of:

- Name
- Address
- Full postal code
- NHS number
- Date of Birth
- Local Identifiers
- Anything else that could identify a service user e.g. photograph, x-ray, dental records etc.

Information that has been anonymised can never be reverted back to its original form.

Information may be used more freely if the subject of the information is not identifiable in any way. When anonymised data will serve the purpose, health professionals must anonymise data to this extent and,

if necessary, take technical advice about anonymisation before releasing data. Whilst it is not ethically necessary to seek consent for the use of anonymised data, general information about when their data will be anonymised should be available to service users.

7.2 Pseudonymisation

Pseudonymisation is sometimes referred to as reversible anonymisation. Patient identifiers, such as name, address or NHS number, are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference. Where those who are using data have no means to reverse the process, and so no way to identify an individual from the data they have, the data may be treated as anonymised and there is no common law requirement to seek consent for their use. For those who have access to both pseudonymised data and the means to reconstitute them, they should be treated as identifiable. The use of pseudonymised data is common in research. As with anonymised data, service users should generally be informed when it is intended that their information will be pseudonymised.

8. Deceased persons

Although the General Data Protection Regulation and the DPA 2018 does not apply to records of deceased persons the ethical obligation to respect a service user's confidentiality extends beyond death. The Information Tribunal in England and Wales has also held that a duty of confidence attaches to the records of the deceased under section 41 of the Freedom of Information Act 2000. If a patient has requested that their information is not disclosed after their death this must be respected. The Access to Health Records Act 1990 gives limited statutory rights of access to those who 'may have a claim' arising out of the death of a deceased patient. Care must always be taken when sharing records of the deceased and advice should be sought in cases of doubt.