HQIP
Healthcare Quality Improvement Partnership

# Information governance in local quality improvement

October 2021


**Update 2021;**

Sasha Hewitt, HQIP
Kim Rezel, HQIP
Desislava Staykovska, HQIP
Poole Hospital NHS Foundation Trust on behalf of N-QI-CAN

**Previous authors:**

Sally Fereday, Healthcare Quality Improvement Partnership
Mandy Smith, Healthcare Quality Improvement Partnership

**Acknowledgements:**

Thank you to Rajoo Veeren from the Office of the National Data Guardian for co ordinating the review of this guide via their Health and Care Information Governance Panel (HCIGP) and working group.

 Design: Pad Creative www.padcreative.co.uk

**Do you need to print this document? Please consider the environment before printing.**

# Contents

# 1 Introduction

## 1.1 What is information governance?

Information governance (IG) is the practical application of the laws and principles that relate to the use of information, especially personal information.

IG protects the rights of the individuals whom personal information is about – referred to as data 'subjects', e.g. patients. It doesn't prevent the use of that information, provided those rights are respected.

Applying the law and rules of IG is a matter of reasonable judgement. Two different judgements might both be reasonable. However, in making judgements, all relevant matters and laws should always be taken into account, the situation evaluated, risks assessed and managed, and decisions and rationale fully documented.

## 1.2 Key legislation and principles

Key legislation and principles applicable to IG in healthcare quality improvement studies:

| | |
|---|---|
| ***Data Protection Act (DPA) 2018*** | An Act of Parliament of the United Kingdom of Great Britain and Northern Ireland which defines UK law on the processing of data on identifiable living people. |
| ***UK General Data Protection Regulations (UK GDPR)*** | A legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the UK. |
| ***Common law duty of confidentiality (see NHS Digital, 2013a)*** | A legal obligation that arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. This duty may be set aside under conditions of legal power, consent, and/or strong public interest. |
| ***Human Rights Act 1998*** | Article 8 of the Human Rights Act is the right to respect for private and family life, home, and correspondence. This right is subject to proportionate and lawful restrictions. It may be set aside for the protection of health or morals, or "for the protection of the rights and freedoms of others". |
| ***Caldicott Principles*** | 8 Principles that organisations should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. When deciding whether [organisations] need to use information that would identify an individual, an organisation should use the Principles as a test. The Principles were extended to adult social care records in 2000. https://www.ukcgc.uk/manual/principles |
| ***Freedom of Information Act (FOIA) 2000*** | Provides public access to information held by public authorities, whereby they must publish certain information about their activities, and members of the public are entitled to request information. |

When undertaking local or regional healthcare quality improvement studies involving personal information it is therefore essential to seek input from your organisational:

- **Data Protection Officer (DPO)** – role is to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority
- **Caldicott Guardian** – the senior person responsible for protecting the confidentiality of patient and service-user information, and enabling appropriate information-sharing
- **Senior Information Risk Officer (SIRO)** – the person with ownership of information risk policy, who acts as an advocate for robust information risk management.

# 2 Purpose of this guide

## 2.1 Scope

This guide describes how IG laws and principles apply to the use of personal data in local or regional multi-agency healthcare quality improvement studies such as clinical audit, productivity reviews, intervention testing, and service evaluation. The two differing approaches are summarised as:

- **Local and national quality improvement studies:** Designed by and taking place within organisations providing direct care, involving one or more organisational teams and departments, focusing on specific local issues, and often following the patient pathway
- **Regional multi-agency quality improvement studies:** Designed by and taking place across different organisations and/or sectors, involving a number of organisational teams and departments, focusing on specific local issues, and often following the patient pathway (see section 8 of this guide)

## 2.2 National clinical audits

National clinical audits carried out by a range of providers for HQIP under the National Clinical Audit and Patient Outcomes Programme (NCAPOP) fall outside the scope of this document. The data sets they use are managed in line with the IG policies and permissions of each national clinical audit provider, for example, through application to the Health Research Authority Confidentiality Advisory Group for Section 251 permission to be able to collect identifiable data in the form of the NHS number. For more information on their specific processes, national clinical audit providers are contactable via the HQIP website: www.hqip.org. uk/national-programmes/a-z-of-nca/.

**Disclaimer:** Due to the dynamic nature of Information Governance readers are advised to seek expert advice and refer to updated national guidance as appropriate. This guidance document does not constitute legal advice. HQIP will highlight changes and update our website with links to national information where appropriate as it becomes available.

## 2.3 Terminology

Under the UK GDPR, 'personal data' means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly. For example; name, address, postcode, date of birth or NHS Number. Health personal information remains confidential after death, and relatives are owed an ethical duty, as well as a legal duty, of respect for private, family life (NHS Digital, 2013a). The terms 'personal data' and 'personal information' are therefore used interchangeably within this guide, except in the context of the DPA.

> Personal data means any information relating to an identified or identifiable living individual; an identifiable person is one who can be identified, directly or indirectly. For example; name, address, postcode, date of birth or NHS number.

# 3 Who is this guide for?

This guide is designed to assist clinicians, quality improvement specialists, support staff, and service users who lead, take part in, or review, local and regional quality improvement studies such as clinical audits, with the application of IG law to their work.

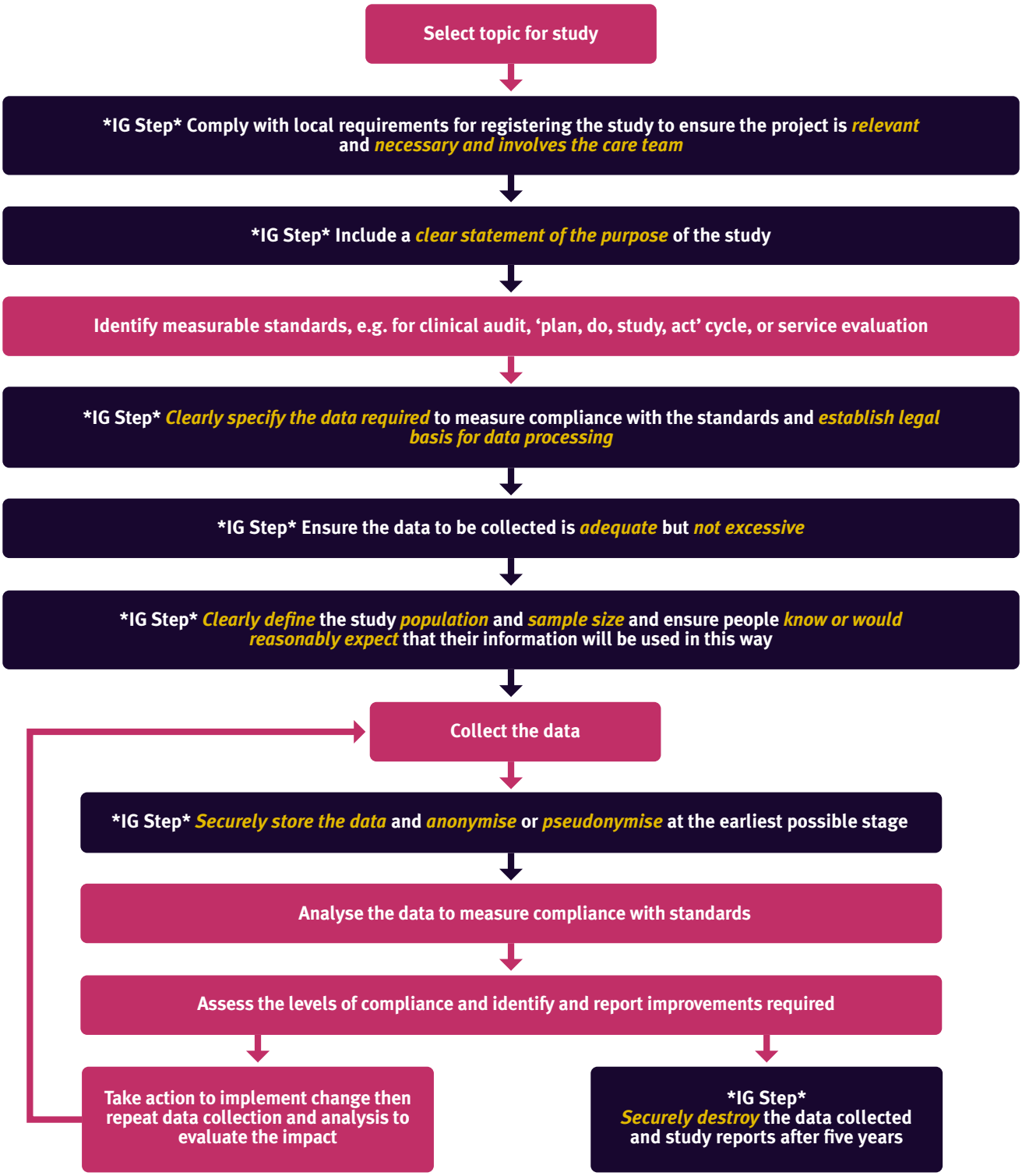
# 4 Information governance in local and regional quality improvement

Numerous stages of the quality improvement cycle require the application of IG law and principles. In the first instance, confirming that a quality improvement study and subsequent health record access are absolutely necessary is key. Clearly defining the purpose of the study, target population, and sample size, helps to ensure that information collected is minimised as far as possible, so that it is adequate but not excessive (see section 5.2 of this guide). Anonymisation or pseudonymisation of information at the earliest possible opportunity, along with secure storage and timely destruction of collected data, are essential to protect personal confidential data throughout a quality improvement study.

The flowchart on the following page provides an overview of the stages of a local or regional quality improvement study along with a number of information governance steps to take along the way.

**Anonymisation** – The process of turning data into a form that does not identify individuals, allowing for much wider use of the information.

**Pseudonymisation** – processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject following disclosure without the use of additional information, provided that such additional information is withheld from the recipient of the disclosed data and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.




**Information governance for local and regional quality improvement studies – an overview**

# 5 The Data Protection Act

The Data Protection Act (DPA 2018) aims to empower individuals (or data subjects) to take control of their personal data and to support organisations (or data controllers) with their lawful processing of personal data. It outlines six data protection principles:

1. Processing must be lawful, fair and transparent
2. Purposes of processing must be specified, explicit and legitimate
3. Personal data must be adequate, relevant and not excessive
4. Personal data must be accurate and kept up to date
5. Personal data must be kept for no longer than is necessary
6. Personal data must be processed in a secure manner

**DPA 2018, Chapter 2, Part 4**

This section of the guide explains six data protection principles, and how they apply to healthcare quality improvement studies.

## 5.1 First data protection principle – Fair, transparent and lawful use

`Processing must be lawful, fair and transparent'

**DPA 2018**

Those processing personal data for quality improvement studies must ensure that people know or would reasonably expect their information to be used in that way. NHS organisations are statutory bodies with the statutory power and duty to provide care. Carrying out a quality improvement study isn't a problem where NHS organisations provide the care they are auditing, and public interest in improvement is strong. They have a statutory duty to provide care and a transparent quality review such as clinical audit is a necessary part of providing that care, and so there is an implied power to do so. Furthermore:

- All healthcare providers and managers registered with the Care Quality Commission have a statutory duty to carry out clinical audits, and to take other quality improvement measures (Health and Social Care Act 2008)
- The www.dsptoolkit.nhs.uk*

The Data Security and Protection Toolkit (DSPT) section 404 previously required organisations to carry out audits of clinical records to ensure their quality and accuracy.

Whilst not an official requirement, it would be good practice for organisation to:

- Have an approved governance approach to auditing clinical records which provides board assurance. This should include an overarching review to:
  - Confirm the need to audit individual clinical specialties
  - Ensure the audit is still relevant, e.g. incorporates move to electronic nursing / medical notes
  - An assessment of risk within specialties including triangulation of incidents and complaints and reviews by external bodies including CQC
  - Ensure it includes priority clinical standards
  - Check regularly for amendments to the DSPT to ensure their governance approach is up-to-date
  - The General Medical Council (GMC) places a professional duty on doctors to `take part in[o] regular reviews and audits of their own work and that of their team' (GMC, 2013)

* The DSPT is reviewed on a yearly basis, the current DSPT version 2 issued in 2018 does NOT outline a requirement to audit clinical records.

Having established that the statutory power and the positive duty are in place to carry out quality improvement studies such as clinical audit, that power must be exercised, and duties discharged, lawfully. Patients can, and do, reasonably expect that personal information about their health will be kept private. There are exceptions, for example, when the information is public knowledge. But it is much safer, and much easier, to treat all healthcare personal information as private and confidential. It is important to note the following:

1. Information need not have been given or received in confidence for it to be confidential, (see Campbell v MGN, 2004)
2. The duty is owed to the person the information is about, and not to anyone who may have shared it, whether in confidence or not

### 5.1.1 Legal basis

Confidential information should only be recorded, used, accessed, or disclosed, if there is a legal basis for doing so. To remain lawful controllers must ensure:

1. An UK GDPR article 6 condition is satisfied (for personal data)
2. An UK GDPR article 9 condition is satisfied (because health data is a special category of personal data)
3. Compliance with the common law duty of confidentiality (which states that information shared in confidence should not be disclosed without the individual's consent)

There are six legal bases under article 6 of the UK GDPR (consent, contract, legal obligation, vital interests, public task and legitimate interests) and 10 conditions for processing specialist category data in article 9.

The Health and Care Information Governance Panel advises that the following would be the most appropriate lawful basis for direct care and administrative purposes, including local clinical audit:

- article 6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…' and 9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'

For common law purposes, local clinical audit is considered an aspect of direct clinical care, therefore implied consent is the common law legal basis often relied on. Patient consent can be implied when personal data about patients is used for their care, including the transparent assessment of that care.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

https://www.nhsx.nhs.uk/information-governance/guidance/use-and-share-information-confidence/

### 5.1.2 National Data Opt Out

**Implied consent** is an assumption of permission to do something that is inferred from an individual's actions rather than explicitly provided.

In May 2018, the national data opt-out was introduced in England which allows a patient to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment. NHS Digital Understanding the national data opt out https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out

All health and adult social care organisations are required to be compliant with the national data opt-out policy, when they are using confidential patient information for purposes beyond an individual's care and treatment. Further information about the deadline for compliance is here: https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out

National data opt-outs apply:

- To the use of confidential patient information approved under Section 251, regulation 2 or regulation 5 (general medical purposes) of the Health Service (Control of Patient Information) Regulations 2002.
- In cases where the approval is subject to the Confidentiality Advisory Group (CAG) 'standard condition' that a patient's wishes regarding use of information about them (i.e. their opt-out) is respected.
- Whenever data are transferred across data controllership boundaries or used for a new purpose.

- Once hospitals have submitted data to your project, having applied the national data opt-out , the national data opt-out will not need to be reapplied by yourselves unless you transfer data to another controller or process data for another purpose.

Please refer to, read and implement, the national guidance at: https://digital.nhs.uk/services/national-data-opt-out to understand requirements and responsibilities to become fully compliant.

NHS Digital provide the 'Check for National Data Opt-out' service to enable organisations to submit lists of NHS numbers to be checked for national data opt-outs with an updated list of NHS numbers being returned for those where no national data opt-out exists. This service can currently be accessed through the Messaging Exchange for Social Care and Health (MESH), more information about these services can be found at: https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out

Implementation and compliance guidance have been issued by NHS digital https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out. Organisations should ensure that where confidential patient information is processed or disclosed, they are clear how the common law duty of confidentiality is being satisfied as this will determine whether the National data opt-out applies.

Local clinical audit. 'The use of personal confidential data for local clinical audit is permissible within an organisation with the participation of a health and social care professional with a legitimate relationship to the patient through implied consent.' National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out

NHS Digital have also confirmed that local clinical audit 'Is outside the scope of the national data opt-out' as detailed in the National Data Opt-out Data Uses Release Compendium v1.3 (updated 27 April 2020) – see link above to the compendium.

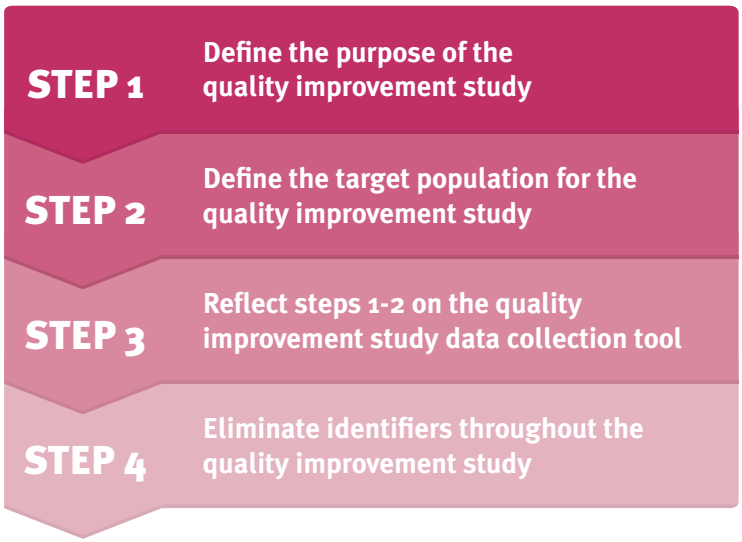
## 5.2 Second data protection principle – Purpose limitation

Personal data accessed through quality improvement study data collection should not be used for any purpose other than that defined within the specific study protocol, and any further processing must be compatible with that purpose.

Data collected for one study could be used for another, in line with this principle. The flowchart on the next page sets out the key steps to take to ensure that data is minimised as far as possible, to keep to defined study requirements.

> Purposes of processing must be specified, explicit and legitimate
>
> **DPA 2018**

# 5.3 Third data protection principle – adequacy and relevance




**Key steps to data minimisation in quality improvement studies**

## Step 1:

The purpose of a quality improvement study needs to be clearly defined, before the information required to meet that purpose can be decided upon. As such the Information Commissioner's Office (ICO) advises, 'to assess whether you are holding the right amount of personal data, you must first be clear about why you are holding and using it. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

## Step 2:

Similarly, the quality improvement study 'target population needs to be clearly and precisely defined' (CRC Press, 2011), as it will be excessive to collect data about patients outside that population.

## Step 3:

The quality improvement study protocol should be very clear about the study purpose and the information required to meet that purpose, and any data collection form, or data collection tool, should reflect this. Data collection forms and tools 'must specify precisely the information to be extracted from the data source, and allow the data collector to indicate clearly whether or not each audit criterion has been met for each record audited.'(CRC Press, 2011) Collecting the right information depends on the precision of the form or tool, and of course it would be excessive to collect the wrong information.

## Step 4:

Eliminate actual identifiers. 'Data collection forms must use an audit number for each record audited, and this should be generated specifically for the audit. This avoids the need for any actual identifiers to be used that could allow service users to be identified.'(CRC Press, 2011) Even though there is the Common Law legal basis of implied consent to access the data in identifiable form, all identifiers should still be removed and if necessary coded at the earliest possible opportunity. Clinicians and other staff can also be de-identified and given coded identities. The use of quality improvement study codes, or audit codes 'enables service-user records to be referred back to in the event of any recording anomalies on the data collection form'. (CRC Press, 2011) It also enables individual patients to be followed up if required, or tracked through time, and for data about them to be linked, without identifying them. Quality improvement study reports and other published results should be anonymised, at least in respect of patient data, to the level required by the Information Standard Board's (ISB) Anonymisation Standard. (NHS Digital, 2018[1])

[1] August 2019: Update: Note that DCB has been made aware of the need to update this information standard to align with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. However, work to update the standard is dependent upon the Information Commissioner's Office (ICO) updating its guidance on anonymisation and as yet there is no firm date for this. As soon as this is published NHS Digital, as developer, will publish further information about the timescales for updating this standard.

> `Personal data must be adequate, relevant and not excessive'
>
> **DPA 2018**

'Collect only what you need' is a basic principle of a quality improvement study or clinical audit, (CRC Press, 2011 and BPP Learning, 2012). This is because:

- 'Careful identification and selection of only the data items necessary for the audit is important to ensure the efficiency and effectiveness of the data collection' (CRC Press, 2011)
- The data minimisation principle, the third principle of the DPA, is that 'personal data shall be adequate, relevant and limited to what is necessary' (DPA, 2018)

Relevance is key. Data that is not relevant for the purposes of a quality improvement study such as a clinical audit will be excessive, and data that omits relevant information will be inadequate. Following steps 1-4 set out within the flowchart at section 5.2 of this guide will help to ensure that you collect only what you need, and can justify your approach.

It should be said, however, that the risks of data being inadequate might outweigh concerns about excessiveness, both in terms of the number of different items of information needed, and the number of patient records that need to be studied or audited. This is an important consideration in determining sample size, whereby a sample of the target population needs to reflect the whole population with sufficient accuracy. (CRC Press, 2011).

## 5.4 Fourth data protection principle – accuracy

> `Personal data must be accurate and, where necessary, kept up-to-date.'
>
> **DPA 2018**

The fourth data protection principle requires that all personal data held is accurate and, where necessary, kept up-to-date. It is unfair to people, and risky, to hold or use data about them that is inaccurate or outdated.

Making sure that data used is accurate and up-to-date, not invalid, insufficient, or misleading, and fact, not opinion, is part of effective practice in quality improvement studies; for example, all data should be up-to-date in accordance with the timeframe of an audit.

## 5.5 Fifth data protection principle – retain only as necessary

> `Personal data must be kept for no longer than is necessary'
>
> **DPA 2018**

The fifth data protection principle is that personal data should be retained for no longer than is necessary and justifiable, for the purposes for which it was obtained. The ICO makes the point that 'ensuring that you erase or anonymise personal data when you no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping you to comply with the data minimisation and accuracy principles, this also reduces the risk that you will use such data in error.' (ICO, 2019)

The NHS Records Management Code of Practice states that clinical audit records should be kept for five years. (NHSX , 2021). https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/

This includes the reports and data collection sheets/exercise. The data itself will usually be clinical so should be kept for the appropriate retention period e.g. data from adult health records would be kept for 8 years.

Ensuring personal data is disposed of when no longer needed reduces the risk that it will become a security/data breach risk and also ensures data will not become inaccurate and out of date. When personal data or de-identified data is destroyed, the ICO's guidance on deletion should be followed.

## 5.6 Sixth data protection principle – security

`Data must be processed in a secure manner'

**DPA 2018**

It is now a legitimate requirement for all data controllers to ensure "security by default and design", which means that appropriate security measures are implemented in all of its functions and processes.

"Organisations must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. They should remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures." ICO, 2019 Some of these measures include usage of encrypted devices and emails, regularly updating existing software and antivirus programmes. There are three key elements of Information Security, also known as the "CIA triad":

- **Confidentiality** – data should only be accessible by authorized and appropriate authority
- **Integrity** – data should be accurate and complete
- **Availability** – data should remain usable and accessible

A personal data breach is a security incident where confidentiality, integrity or availability of personal data has been compromised. Examples of such incidents include unauthorized reversal of pseudonymised data, sending personal data to the wrong recipient or IT systems becoming infected with viruses.

After a notable breach with NHS falling victim to WannaCry ransomware attack in 2017, it became particularly clear how important keeping IT systems secure and up-to-date is.

Security measures may vary from organization to organization and the considerations as to what is appropriate lie with the purpose, type and scope of the processing and the risks it presents, accordingly.

One of the measures recommended for projects that involve processing of personal data, is the Data Protection Impact Assessment, or DPIA. Information Commissioner Office talks about DPIA in further detail here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

## 5.7 Data Subjects Rights

It is important for all organizations acting as data controllers to be aware of individuals' rights under the General Data Protection Regulation and a responsibility to both inform individuals of those and ensure there are mechanisms in place to act on them. There are eight rights to consider:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

**The right to be informed** as to how individual's personal data is collected and used is a key transparency principle under the UK GDPR. Processing of data must be lawful, fair and transparent. Privacy information must be provided prior to data collect or at the moment of data collection so individuals can make an informed decision about if they wish to share their personal data.

An organization performing a local clinical audit must provide individuals with information regarding: purposes for processing of personal data, lawful processing condition, types of personal data to be processed, retention periods for that personal data, who it will be shared with, if their data will be used in a national audit, the level of anonomysation data will receive . ICO provides guidance on delivering the right to be informed.

Healthcare organisations are required to have a publicly available patient privacy notice that outlines patients data subject rights including the purposes of outlining the transparency principle under UK GDPR, fair processing of personal data, lawful processing conditions, data opt out and processing of data.

Within the Healthcare organisation, patient information (data) for local clinical audit is pseudo anonymised or anonymised and is collected under the auspices of fair processing and the patient privacy notice.

### The Right of Access

DPA 2018 and UK GDPR provides data subjects with the right to access to their data. Data subjects can request access to their data in writing or verbally. There must be a process in place to provide the requested data within the time limit of 1 month. The data subject must be provided with; confirmation that you are processing their personal data and a copy of their personal data in an accessible format. An individual is only entitled to their own personal data, and not to information that could identity other people (unless the information is also about them, they are acting on behalf of someone or they have permission to receive this personal data). In most cases a subject access requests will be free of charge to the data subject.

Guidance on Subject Access Requests is available on the NHSX Portal https://www.nhsx.nhs.uk/information-governance/guidance/subject-access-requests/

# 6 Caldicott Principles

A review was commissioned in 1997 by the Chief Medical Officer of England after concerns about the ways in which patient information was being used, and the need to ensure that confidentiality is not undermined. Concerns included information technology developments, and the capacity to disseminate information about patients rapidly and extensively. A committee was established under the chairmanship of Dame Fiona Caldicott, principal of Somerville College, Oxford, and previously president of the Royal College of Psychiatrists. Its findings were published in December 1997. The Caldicott Report highlighted six key principles, and in 2012, Dame Caldicott produced a follow up report, with the addition of a seventh principle. Clearly, all of the Caldicott Principles, (Department of Health, 2013a) summarised below, should be taken into account throughout the healthcare quality improvement study cycle.

## 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 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 but is enough 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.

**8. Inform patients and service users about how their confidential information is used**
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

# 7 Freedom of information

The Freedom of Information Act 2000 (FOIA) covers any recorded information held by a public authority. All NHS organisations are public authorities. FOIA provides access to information in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

The ICO expects NHS organisations to publish 'audit reports delivered at board/governing body level' as part of their publication schemes. (ICO, 2014c) Published reports should be anonymised, at least in respect of patient data, to the level required by the ISB's Anonymisation Standard. This is relevant for any unpublished reports and other audit data disclosed following a request for information. However, the position can be slightly different for clinicians and other staff working in their professional capacity, and the ICO's guidance on this should be followed. (ICO, 2013) Model publication scheme guidance here.

The FOIA doesn't give people access to their personal data, but requests for such access can be made under Data Protection Act 2018 as a Subject Access Request.

Organisations should have a FOI policy which provides guidance on what the legal obligations are on how to respond to a request.

The guidance should cover:

- How to recognise a request
- How to assist member of public in validating their request
- Who in the orginisation notify of a request
- How long orginisation has to respond to a request (20 working days)
- Possible exemptions

More detailed guidance is provided by the ICO.

# 8 Regional multi-agency teams

Regional multi-agency quality improvement studies can be carried out in a variety of ways, e.g.:

Individual organisations may study the services they provide, and then collaborate with other organisations to compare and assess findings, without the need for any exchange of confidential patient-level data

Studies may follow patient journeys over time, reviewing the person-centred integrated care of patients, and the care given by a multi-agency team across different locations, whereby patient-level data is shared

Studies may review joint multi-agency patient care at one point in time, whereby patient-level data is shared

There is a legal requirement to conduct a DPIA when processing medium to high risk personal or processing personal data In a new way or implementing new technology to process data. Controllers should be clear how the common law duty of confidentiality is being satisfied and it is good practice to have an information sharing agreement in place, as part of the study protocol. A template is available on the NHSX Portal at: https://www.nhsx.nhs.uk/information-governance/guidance/data-sharing-agreement-template/. It should include the following points, which have been covered by this guide (ICO, 2017e):

- Purpose of the quality improvement study and need to share
- Statutory power/duty and legal basis (implied consent)
- Information that will be shared
- Organisations that will be involved
- Fair processing information that should be given
- Measures that should be taken to ensure adequate security
- Restrictions on further disclosure
- Arrangements for responding to FOI requests and DPA subject access requests
- Agreed retention periods
- Processes to ensure secure information deletion
- Data protection breach procedure

NHS x has recently published its Information Governance Framework for Integrated Health and Care: Shared Care Records - a new guide which provides information on sharing personal or confidential patient information between health and social care bodies across geographical boundaries for the individual care of patients or service users. (https://www.nhsx.nhs.uk/information-governance/guidance/summary-of-information-governance-framework-shared-care-records/information-governance-framework-for-integrated-health-and-care-shared-care-records/). In addition the Health and Social Care (Safety and Quality) Act 2015 (www.legislation.gov.uk/ukpga/2015/28/contents/enacted) places a legal duty on health and social care providers to share information where this may facilitate the provision to the individual of health (or social care) services in England, and is in the individual's best interests. There is no obvious reason why 'organisational boundaries' should not include 'boundaries' between primary and secondary care. www.gov.uk/government/news/safer-care-for-patients

We have already seen that 'sharing for direct care' includes disclosures for clinical audit purposes.

It follows that members of multi-agency care teams can rely on implied consent to share confidential patient information with each other for the purposes of clinical audit and other quality improvement studies. That means they don't have to de-identify data after collection to the level required for 'limited access anonymisation', (ICO, 2012) but de-identification is still desirable.

However implied consent would not apply to audit or other quality improvement projects for secondary purposes or where the information is required by people outside of the care team. In these circumstances the common law duty of confidentiality must be satisfied either by explicit consent or an alternative legal basis (such as an approval under section 251 of the NHS Act (2006))

However, there is a significant difference between sharing data from patient records and granting access to them. As Caldicott 2 points out, 'a professional in a particular field, such as a physiotherapist treating a patient's knee, may not need to know about his impotence'. (Department of Health, 2013c) Moreover, the patient would not expect the physiotherapist to be given access to that information, and so his consent could not be implied.

So, if access cannot be restricted to information within the scope of the care being studied, or if the study is of whole records, members of multi-agency teams should collect patient-level personal information from their own organisations only. Identifiers should in any event be removed from information before it is entered into a data collection form using a quality improvement study code, or audit code, so that it can be linked to data about the patient from other organisations in the care team.

It is important to build public trust in the management and control of personal data.

# 9 Benchmarking

Benchmarking through quality improvement studies such as clinical audits enables the comparison of standards of care attained by teams or organisations of the same type, locally or regionally. In terms of IG, benchmarking should be straightforward, as the results of local and regional quality improvement studies and audits are anonymised, aggregated, and then compared.

# 10 Commissioners and other non-care providers

NHS Digital states:

> `Commissioning Support Units (CSUs) and Clinical Commissioning Groups (CCGs) can only receive patient confidential data if there is a clear legal basis for them to do so. In general, they are not allowed to receive patient confidential data.' (NHS Digital 2017b)

This is supported by Caldicott principles2, which details that there are 'only a small percentage of situations' in which commissioners can properly require access to personal confidential data (Department of Health, 2013c). As part of the IG review, commissioners explained that they wanted access to confidential personal data to check the quality of care at every stage of a patient pathway, as the individual moves among a series of health and social care providers. They suggested that the surest way of doing this was to look at a sample of personal files. However, the review panel concluded there did not appear to be a robust case for commissioners holding personal confidential data, and any exceptions should be argued on an individual case-by-case basis. (Department of Health, 2013c).

The panel suggested that an alternative would be to ask for the data that demonstrates effectiveness. Another alternative, if different providers were commissioned across the care pathway, would be for the commissioner to commission audit reports on the whole care pathway from the local health and social care professionals who have a legitimate relationship to the patient. (Department of Health, 2013c)

It should be added that the NHS Standard Contract states that 'the commissioner may at any time appoint an auditor to conduct an objective and impartial audit of the quality and outcomes of any service'. (NHS England, 2021) The auditors will be agents of the commissioners, and so will be bound by any constraints on the commissioners. Commissioners should note that the practice of giving temporary contracts to the employees of commissioners so that they can access personal data for audit purposes is outside the scope of implied consent – it is not what patients expect.

However, commissioners do have a duty to 'exercise their functions with a view to securing continuous improvement in the quality of services'. (NHS, 2013a) Therefore, where necessary, e.g. where healthcare providers are failing in the review and maintenance of the quality of care they provide – posing serious risks to the safety, health and wellbeing.

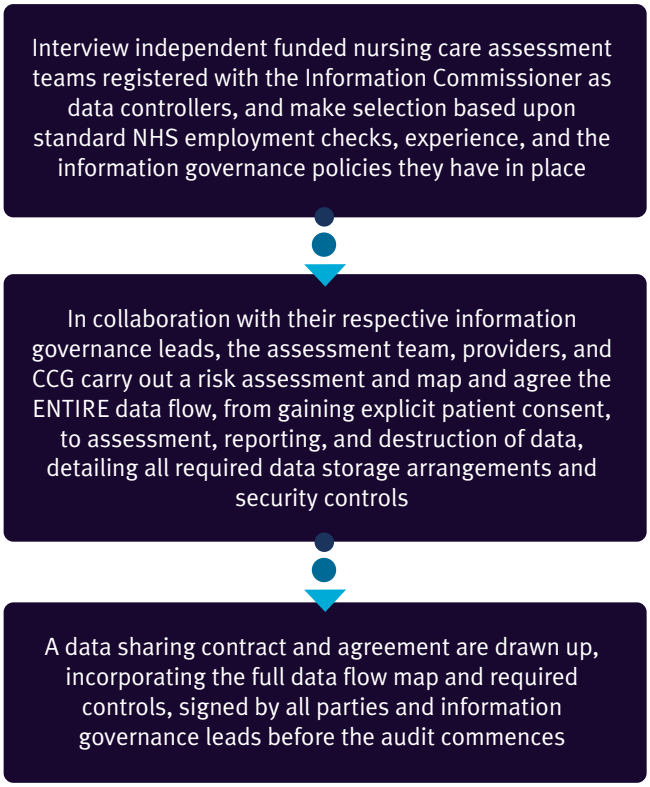
of patients – healthcare quality improvement leads within commissioning organisations might formally examine health records directly, or through an intermediary organisation, with explicit consent from patients and all the necessary controls in place as per the case example and flowchart below.

**Case example: CCG review of funded nursing care packages**

A CCG identified risks to patients who were receiving unsatisfactory funded nursing care packages, for which it appeared they had been inadequately assessed by healthcare providers before discharge into the community.

Patients were felt to be at risk of receiving inadequate care, while millions of pounds of resources were spent on care packages that did not appear to be routinely reviewed for their suitability.

As requests for evidence of improvement from providers were fruitless over a 12-month period, the CCG felt it necessary to carry out an independent audit of funded nursing care packages, requiring health record access with patient consent, implementing IG controls as summarised within the flowchart opposite.

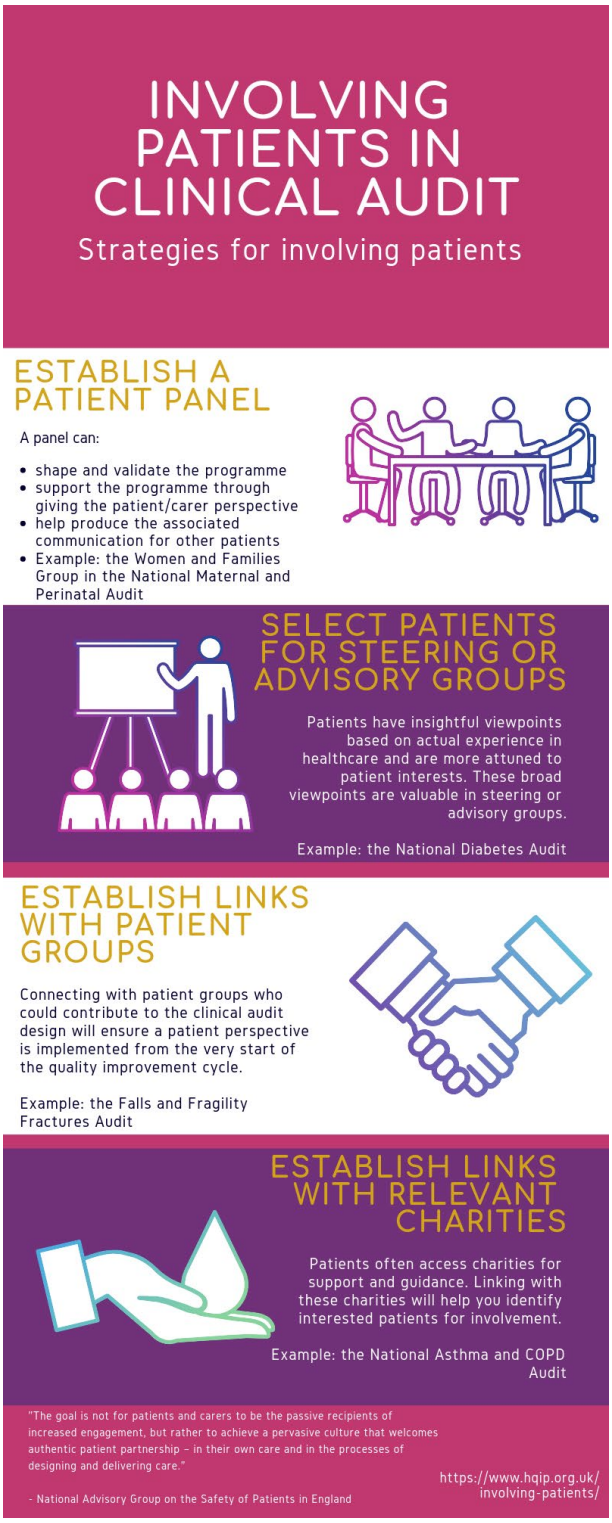



When undertaking a "clinical audit, productivity reviews, intervention testing, and service evaluation" project of a healthcare provider or NHS organisation, commissioners and other non-care providers should at the earliest opportunity work with the responsible officer within the organisation, e.g. Caldicott Guardian and Head of Governance. This is to ensure that appropriate organisational and national approvals are in place for the project and ensures that the use of patients data is appropriate and safeguarded.

# 11 Patient and public involvement

All quality management systems require the service user voice in order to identify shortfalls in service provision and make necessary improvements. NHS England's publication, www.england.nhs.uk/publication/patient-and-public-participation-in-commissioning-health-and-care-statutory-guidance-for-ccgs-and-nhs-england/ Patient and public participation in commissioning health and care: Statutory guidance for clinical commissioning groups and NHS England (NHS England, 2017) describes the importance of engaging with patients, carers and the public when redesigning or reconfiguring healthcare services.

> `Staff can better understand population health needs, and respond to what matters most to people when they involve and listen to those who need, use and care about NHS services. Patients and the public can often identify innovative, effective and efficient ways of designing, delivering and joining up services.'
>
> **NHS England, 2017**




**HQIP, 2019**

Healthcare organisations must comply with the law and good practice when involving patients and the public in clinical audit; it is therefore essential to consult your organisational IG lead, to ensure compliance as well as assist with a privacy impact risk assessment, (ICO, 2014b) and to seek the approval of your Caldicott guardian and Senior Information Risk Officer (SIRO) for such studies.

Many healthcare organisations have set up a patient panel to support clinical audit activity. It should be remembered that panel members should not be involved in collecting data from patient health records. However, data collection represents just one step in the entire quality improvement cycle and patients and the public can contribute to topic selection, the planning and design of clinical audit projects, the analysis and review of results, and the planning and implementation of improvements, without the need to see the personal confidential information of individual patients through health record review.

Personal confidential data – including a patient's health record – can only be disclosed under certain specific circumstances. Patients must give consent to their personal confidential data being disclosed to anyone other than:

- Those who provide direct care
- Employees of the care provider accessing that information as part of their designated role

It should be noted that agreements such as honorary contracts between organisations and panel members (even with confidentiality clauses) cannot provide a legal basis for panel member access to health and other confidential information. The legal basis for that may be one of the following; the explicit consent of the individual, the best interests of the individual or a statutory provision such as support under s251 of the NHS Act (2006).

When patient panel members invite other patients to give their views on their treatment and experience through surveys or interviews, it must be made clear to those patients that they are under no pressure to participate, and that participation is on a purely voluntary basis. Where patient panel members collect data through surveys or interviews, any patient, service user, carer, or staff member completing the survey or undergoing interview should be:

- Informed of the content of the survey or interview
- Informed of the purpose of the study
- Invited to take part in the study, if they would like to do so
- Asked to consent to their involvement, and to the sharing of their anonymised responses

Panel members should be required to withdraw if they recognise a patient.

For effective healthcare quality improvement it is important to involve and gather the views of a range of service users, including those from vulnerable groups. Consent for the involvement of a child (aged under 13) as a panel member or as a patient must be obtained from a person with parental responsibility. In addition, adults, who lack the mental capacity to decide to be involved as a panel member, or as a patient, should only be involved in liaison with their advocate, in line with the Mental Capacity Act 2005.

All involved in healthcare quality improvement studies should undergo IG training, receive appropriate security clearance, and read and sign a confidentiality agreement. Training should meet the organisation's IG Toolkit requirements to level 2.

Organisations should ensure that they have insurance for the risks of panel member involvement, covering information security risks, and should carry out a privacy impact assessment (ICO, 2014b) for each clinical audit.

Further information is available within HQIP's publications Patient and public involvement in quality improvement, (HQIP, 2016a) and Developing a patient and public involvement panel for quality improvement (HQIP, 2016b), available on the HQIP website.

# 12 Further reading

Further useful information sources include:

- The NHSX IG Portal which publishes guidance on behalf of the Health and Care Panel: www.nhsx.nhs.uk/information-governance/
- Information Commissioners Office (ICO) for authoritative DPA and FOIA guidance: www.ico.org.uk/
- Health Research Authority Confidentiality Advisory Group: www.hra.nhs.uk/about-the-hra/our-committees/section-251/
- NHS Constitution: www.gov.uk/government/publications/the-nhs-constitution-for-england/

# References


1. Arnstein, Sherry, R, 1969. A Ladder of Citizen Participation. (Journal of the American Planning Association)
2. BPP Learning, 2012. Clinical Audit for Doctors and Health Care Professionals, Chapter 2
3. Campbell v MGN [2004] UKHL 22: www.publications.parliament.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm
4. CRC Press, 2011. New Principles of Best Practice in Clinical Audit pages 61, 63 and 65-68
5. Data Protection Act, 2018.: www.legislation.gov.uk/ukpga/2018/12/contents/enacted
6. Department of Health, 2013a. Information: To share or not to share; Government response to the Caldicott review. www.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF
7. Department of Health, 2013b. The Information Governance Review: paragraphs 3.13 and 3.3 respectively: www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
8. Department of Health, 2013c.The Information Governance Review, paragraphs 3.3, 3.7 and 7.3.2: www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
9. Freedom of Information Act, 2000: www.legislation.gov.uk/ukpga/2000/36/contents
10. General Medical Council (GMC), 2009. Confidentiality guidance paragraph 30: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality
11. GMC, 2013. Good Medical Practice paragraph 22: www.gmc-uk.org/static/documents/content/GMP_.pdf
12. Health and Social Care Act, 2008 (Regulated Activities) Regulations 2010, regulation 10: www.legislation.gov.uk/ukpga/2008/14/contents
13. Health and Social Care (Safety and Quality) Act 2015: www.legislation.gov.uk/ukpga/2015/28/contents/enacted
14. HQIP, 2016a. Patient and public involvement in quality improvement: https://www.hqip.org.uk/resource/a-guide-to-patient-and-public-involvement-in-quality-improvement/
15. HQIP, 2016b. Developing a patient and public involvement panel for quality improvement:https://www.hqip.org.uk/wp-content/uploads/2018/02/developing-a-patient-and-public-involvement-panel-for-quality-improvement.pdf
16. Human Rights Act 1998: www.legislation.gov.uk/ukpga/1998/42/contents
17. Information Commissioner's Office (ICO), 2011. Data sharing

code of practice: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/

18. ICO, 2012. Anonymisation: Code of Practice, page 37: www.ico.org.uk/media/1061/anonymisation-code.pdf

19. ICO, 2013. Requests for personal data about public authority employees: www.ico.org.uk/media/for%20%20organisations/documents/1187/section_40_requests_for_personal_data_about_employees.pdf

20. ICO's guidance on deleting data available here: www.ico.org.uk/your-data-matters/online/deleting-your-data-from-computers-laptops-and-other-devices/

21. ICO Conducting Data Protection Impact Assessments: www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

22. ICO, 2014c. Freedom of Information Act 2000 Definition Document for Health Bodies in England: www.ico.org.uk/media/for-organisations/documents/1220/definition-document-health-bodies-in-england.pdf

23. ICO, 2016a. Privacy notices code of practice: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

24. ICO, 2016b. FOIA schemes (ICO): www.ico.org.uk/for-organisations/guide-to-freedom-of-information

25. ICO. The amount of personal data you may hold: www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

26. ICO. Retaining personal data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

27. ICO. Information security. www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

28. NHSx Subject Access Request: https://www.nhsx.nhs.uk/information-governance/guidance/subject-access-requests/

29. ICO, 2017e Data sharing checklists: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/annex-a-data-sharing-checklist/

30. NHS Digital, 2017a. Anonymisation Standard for Publishing Health and Social Care Data. ISB 1523: www.digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/isb1523-anonymisation-standard-for-publishing-health-and-social-care-data

31. Mental Capacity Act 2005: www.legislation.gov.uk/ukpga/2005/9/contents

32. National Data Guardian, 2016. Review of data security, consent and opt-outs: https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

33. NHS England, 2013b: Transforming Participation in Health and Care www.england.nhs.uk/2013/09/trans-part/

34. NHS England, 2017. NHS Standard Contract 2021/22: https://www.england.nhs.uk/nhs-standard-contract/21-22/

35. NHS Digital, 2013b. A guide to confidentiality in health and social care: references page 28: www.content.digital.nhs.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

36. NHSx, 2021. IG Framework for integrated health and care: Shared Care Records, https://www.nhsx.nhs.uk/information-governance/guidance/summary-of-information-governance-framework-shared-care-records/information-governance-framework-for-integrated-health-and-care-shared-care-records/.

# Appendix 1 – Privacy Notice

UK GDPR provides individuals with the right to be informed about the collection and use of their personal data. This provides transparency, a key component of UK GDPR. This gives individuals the opportunity to make informed decisions about the way they allow their data to be used.

Privacy notice/information must be provided to individuals at the time you collect their personal data. Privacy information must be; concise, transparent, intelligible, easily accessible, and it must be presented in clear and plain language.

Please take the special needs of individuals into account. You must regularly review, and where necessary, update your privacy information.

Privacy Notice must include the below information.

| What information do we need to provide? | Personal data collected from individuals | Personal data obtained from other sources |
|---|---|---|
| The name and contact details of your organisation | ✓ | ✓ |
| The name and contact details of your representative | ✓ | ✓ |
| The contact details of your data protection officer | ✓ | ✓ |
| The purposes of the processing | ✓ | ✓ |
| The lawful basis for the processing | ✓ | ✓ |
| The legitimate interests for the processing | ✓ | ✓ |
| The categories of personal data obtained | | ✓ |
| The recipients or categories of recipients of the personal data | ✓ | ✓ |
| The details of transfers of the personal data to any third countries or international organisations | ✓ | ✓ |
| The retention periods for the personal data | ✓ | ✓ |
| The rights available to individuals in respect of the processing | ✓ | ✓ |
| The right to withdraw consent | ✓ | ✓ |
| The right to lodge a complaint with a supervisory authority | ✓ | ✓ |
| The source of the personal data | | ✓ |
| The details of whether individuals are under a statutory or contractual obligation to provide the personal data | ✓ | |
| The details of the existence of automated decision-making, including profiling | ✓ | ✓ |

# Your personal information

## The leaflet should give the full name and contact details of your organisation

## How we record and use information about you and the care you receive in our (hospital / clinic / service)

### Using information to keep you safe

In the NHS we aim to provide you with safe and effective healthcare. To do this we must keep records about you, your health, the care we provide to you and how we use you personal data to do this. Under the Data Protection Act, we are legally required to make sure that the personal information we hold about you is only used in a fair and lawful way.

Your care is recorded in paper notes and electronic systems that are secure. The people who provide your care will use this information to treat you safely. We may also share this information with others who provide you with care – for example **we will tell your GP about the care you have received in the hospital.**

### Using information to improve our services

We would like to be able to use the information held within your records to help improve the services that we provide. We can do this by collecting information from the records of groups of patients who have similar conditions or have received similar treatments, and comparing this with what we know are the best standards of care. This helps us to identify areas where we need to make improvements. For example, **if we find that some patients are waiting too long to be seen in a particular clinic, we can try to change the appointment system or increase the number of clinic appointments we have available**.

This process of checking care records against best practice is known as clinical audit. It is usually carried out by the staff who have provided you with care, or by support staff who work closely with them. They will only collect your personal identifiable information (e.g. your name, or date of birth, or postcode) if it is necessary. For example, they may need to make sure that they are collecting the correct information about the same patient from different sources, such as **your paper clinic records and your electronic records of blood tests**.

Any information that could identify you as an individual will be removed from the record of the clinical audit as soon as it is possible to do so. Reports of clinical audits may be shared with the management of the **(hospital/service/etc.)** and others, but only after information that could identify you or any other patient has been removed. The record of the clinical audit will be protected by NHS security measures such as computer passwords to limit access, and destroyed after five years.

There are other ways in which the information that we collect about your care can be used to help us improve our services, but we will always keep any information that could be used to identify you as an individual confidential.

Many patients welcome the opportunity to contribute towards improving services:

***"As a patient I have a responsibility to support our healthcare services and I am happy to know that my unique experiences of care will help to improve the quality of care for everyone."***

**Quote from a member of the HQIP Service User Network**

### Other ways in which you can help to improve our services

**(Insert information and contact details for the local patient panel or other patient involvement opportunities.)**

### Regional and national clinical audit

Clinical audits are sometimes carried out by groups of healthcare organisations working across a geographical region. If information is to be shared in this way, any information that identifies you will be removed.

National clinical audits compare the quality of care across many organisations with national standards. The results of these national projects can be used locally to improve services, and nationally to set healthcare policy. The way in which information is collected and held by these national projects varies. If you would like to know more, please ask a member of your care team. They can let you know if your information is likely to be used.

### Your information, your rights

The Data Protection Act gives everyone rights in respect of the data that organisations hold about them. There are rights that apply to all kinds of information and all kinds of organisations, such as the right to see information that is held about you. You also have a specific right to object if you do not want your healthcare records to be used for anything other than direct care. This means you can opt out of having your records used to improve services at a local, regional, or national level.

**If you wish to opt out**, you will be asked to complete a form, which will be placed on your medical record to ensure your wishes are respected. **(The opt out form should be designed in a way that is compatible with all of the information recording and processing systems used by the organisation, and reversible should the patient change their mind.)** You can change your mind at any time, and your decision will not affect the care you receive.

### Complaints

You have the right to complain about any use of your information by the NHS. Complaints should be directed to:
**(Insert complaints department contact details.)**

### Where can I find out more?

If you would like to find out more about clinical audit, the use of information in improving healthcare, or how patients and the public can be involved in healthcare improvement, please visit the Healthcare Quality Improvement Partnership website: www.hqip.org.uk

If you would like to find out more about your rights under the Data Protection Act, please visit the Information Commissioners Office website: www.ico.org.uk/for-the-public/

If you have any questions or concerns about the way the NHS may use your information, please speak to any member of your care team, or contact us directly.



Further information is available at: www.hqip.org.uk

ISBN NO 978-1-907561-54-2

E communications@hqip.org.uk

www.hqip.org.uk

Registered Office: 70 Wimpole Street, London W1G 8AX

Registration No. 6498947

Registered Charity Number: 1127049



October 2021