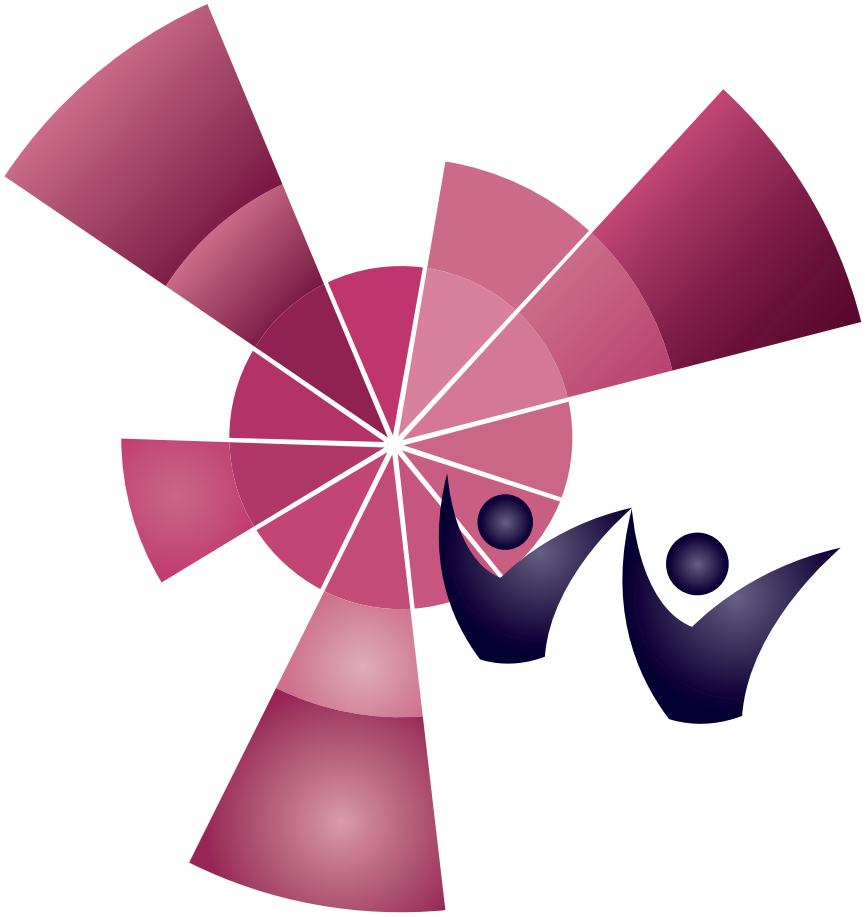
HQIP
Healthcare Quality Improvement Partnership

Information governance in local quality improvement



June 2017

Information Governance Alliance IGA

Authors:

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

Next review:

June 2018

Acknowledgements:

This guide was developed with input from NHS England, NHS Digital, HQIP Service User Network (SUN), the National Quality Improvement and Clinical Audit Network (NQICAN), and the Information Governance Alliance (IGA) – a partnership of the Department of Health, NHS Digital, NHS England, and Public Health England.

 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. Application of these laws and principles in practice can be difficult, but they are, for the most part, straightforward, sensible, and intuitive.

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) 1998	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.
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 (see Department of Health, 2013a)	A number of general principles that health and social care organisations must apply to patient information handling and protection.
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.

Person identifiable data – Person identifiable data is that which can enable a particular person to be identified, for example, their name, address, postcode, date of birth, or NHS number.

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

- **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 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 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/*.

2.3 Terminology

Under the *Data Protection Act (DPA) 1998*, 'personal data' is recorded information about identifiable living people – however, 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.

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

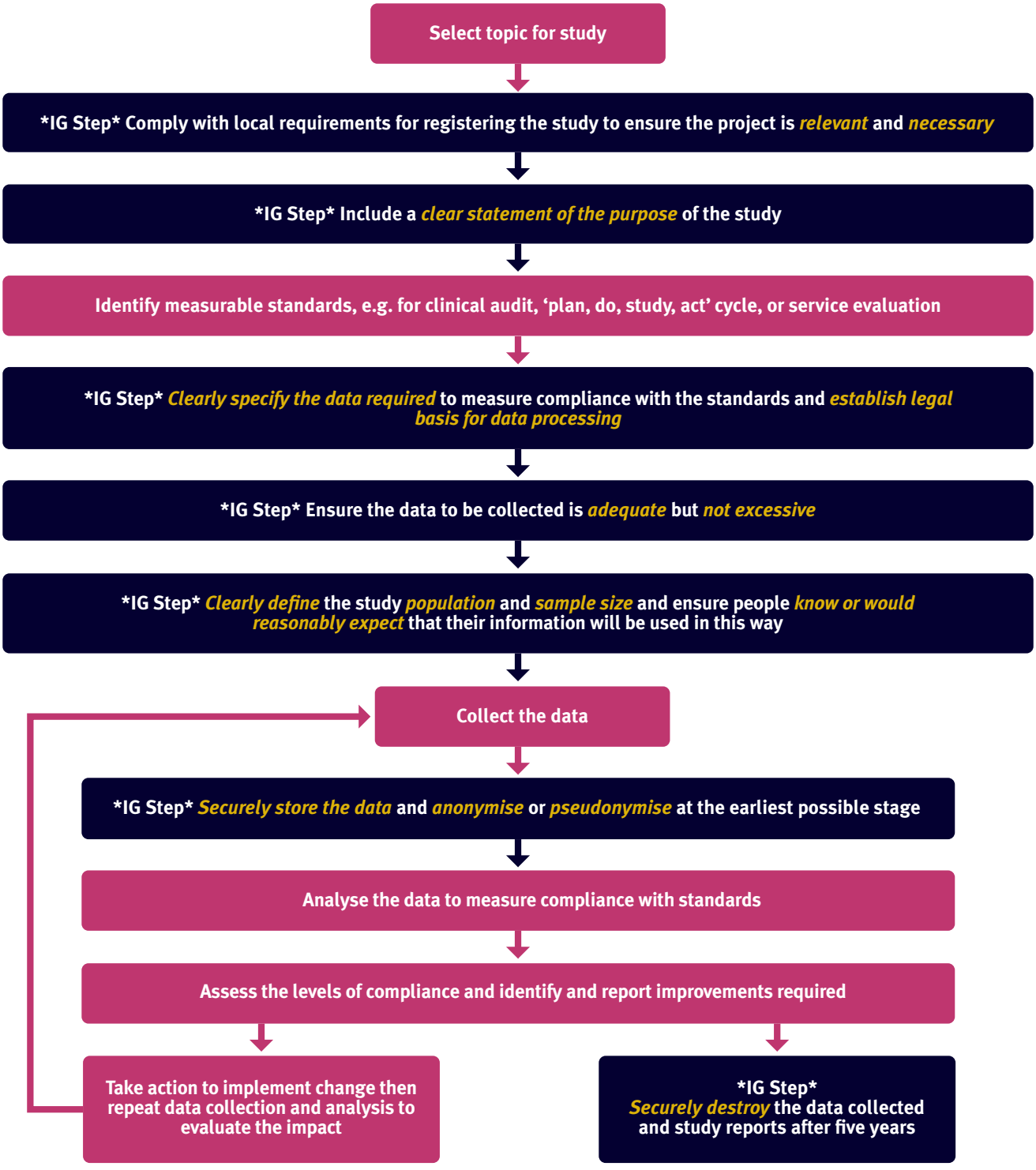
Numerous stages of the quality improvement cycle require the application of IG law and principles. In the first instance, confirming that a quality improvement study and subsequent health record access are absolutely necessary is key. Clearly defining the purpose of the study, target population, and 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 (coding) 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 IG 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 – The process of distinguishing individuals within a dataset using a unique identifier such as a code or number, which does not reveal their real-world identity.

De-identification – The process of ensuring that data cannot be used to identify an individual, either directly or indirectly.



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

5 The Data Protection Act

The *Data Protection Act (DPA 1998)* is based on fair use of personal data. That means being open with data subjects around the use of their data, and ensuring that personal data is handled in line with eight data protection principles, which ensure that it is:

1. Used fairly and lawfully
2. Used for limited, specifically stated purposes
3. Used in a way that is adequate, relevant and not excessive
4. Accurate
5. Kept for no longer than is absolutely necessary
6. Handled according to people's data protection rights
7. Kept safe and secure
8. Not transferred outside the European Economic Area without adequate protection

DPA 1998

The Information Commissioner's Office calls the third, fourth and fifth data protection principles of the DPA 'information standards principles', however this section of the guide covers all eight data protection principles, and how they apply to healthcare quality improvement studies.

5.1 First data protection principle – fair and lawful use

'Personal data shall be processed fairly and lawfully'

DPA 1998

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 *NHS IG Toolkit** requires organisations to carry out audits of clinical records to ensure their quality and accuracy; as the toolkit is updated so should organisations ensure that they follow the latest requirements
- The *General Medical Council (GMC)* places a professional duty on doctors to 'take part in... regular reviews and audits of their own work and that of their team' (GMC, 2013)

* Please note that the IG toolkit is changing and new training materials are also being developed. Please keep up to date through this link – www.igt.hscic.gov.uk

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. Personal information is private and confidential if the person it is about can have a reasonable expectation of privacy in respect of it, (see Campbell v MGN, 2004). Fair information processing is covered in more detail at *section 5.6* of this guide. 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 three things:

1. The test for whether personal information is confidential in common law or private under the Human Rights Act is now the same thing – is there a reasonable expectation of privacy?, (see Campbell v MGN, 2004)
2. Information need not have been given or received in confidence for it to be confidential, (see Campbell v MGN, 2004)
3. 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 Consent

Confidential information should only be recorded, used, accessed, or disclosed, if there is a legal basis for doing so. The legal basis commonly relied on by quality improvement projects such as local or regional clinical audits is implied consent. Patient consent can be implied when personal data about patients is used for their care, including the transparent assessment of that care.

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

The *NHS IG Toolkit* states (Department of Health, 2017):

> *'It is generally accepted that consent can be implied where the purpose is directly concerned with an individual's care, or with the quality assurance of that care, and the disclosure should not reasonably surprise the person concerned .'*
>
> **Department of Health, 2017**

NHS Digital (formerly the Health and Social Care Information Centre (HSCIC)) confirms that direct care includes 'the local audit of the quality of care provided'. (NHS Digital, 2013b)

5.1.2 Data access and use

It may be that the data required for a quality improvement study or a clinical audit can be downloaded electronically in anonymised or pseudonymised form. However, this is still more the exception than the rule – it is more likely, especially if the study is retrospective, that data will have to be collected from a variety of sources in a variety of forms, and that it might be held on paper and/or electronically.

Raw data (sometimes called source data or primary data) are data obtained that have not yet been processed for use.

Collected data is normally anonymised or coded for analysis and assessment, but the collection of data usually entails access to it in its raw state. The GMC state:

> *'If an audit is to be undertaken by the team that provided care, or those working to support them, such as clinical audit staff, you may disclose identifiable information.'*
>
> **GMC, 2009**

This means that clinical audit support staff employed to carry out clinical audit can access patient personal data for audit purposes. **However**, Caldicott 2 states that:

> *'The use of personal confidential data for local clinical audit is permissible within an organisation with the participation of a health or social care professional with a legitimate relationship to the patient through implied consent'*
>
> **Department of Health, 2013b**

This suggests that at least one professional who provided the care should be involved in the audit, though not necessarily in the collection of data. There seems to be considerable latitude here, but good practice is for the care team to carry out the collection of personal data, and any assessment of it while it is still in the form of personal data. There are two reasons for saying that:

1. Caldicott 2 (Department of Health, 2013b) recommends that unregulated staff should be supervised and 'have only necessary and very limited access to patient and client data'
2. Patients will expect that their care team will be directly involved in audit

Remember the IG Toolkit's cautionary advice that '*disclosure should not reasonably surprise the person concerned*'

In any event, quality improvement staff, audit staff, and other specialists can usually provide advice and support to clinicians without the need for them to see any personal data.

It will often be desirable to maintain the involvement of a practitioner who has moved on. In such cases, an organisation-to-organisation letter of authority – rather than an honorary contract, which has no legal leverage – should be used. (IGA, 2015a)

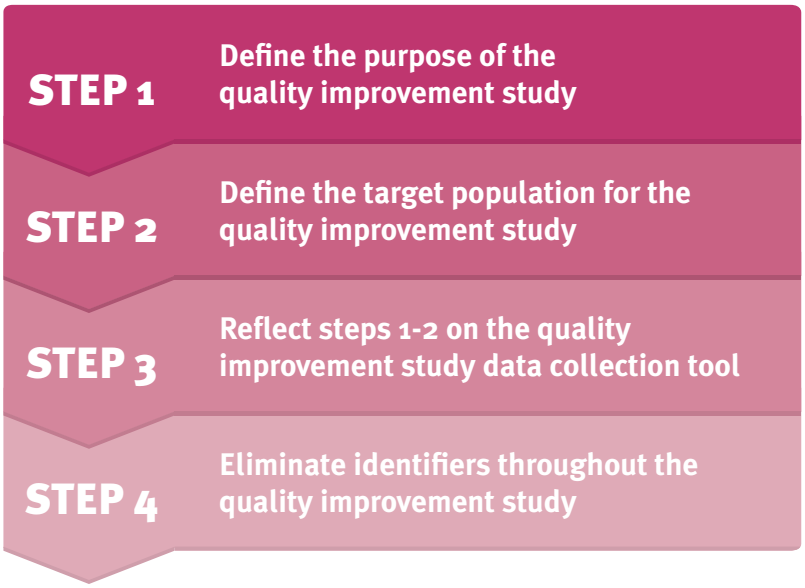
It should be noted that consent to allow access to data cannot be implied if a patient has objected and objections should be invited and clearly visible in a patient's records, see Appendix 1 (National Data Guardian, 2016) If the records are diverse or extensive this might be difficult to achieve, though it is still necessary (NHS Digital, 2015), and essential in order to meet the needs of the *NHS Constitution*.

A patient's objections must be upheld and prominently seen within their records.

5.2 Second data protection principle – use only as specified

> *'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.'*
>
> **DPA 1998**

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.



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.' (ICO, 2017a)

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 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, because consent cannot be implied for unnecessary access to or use of confidential personal information. 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, 2017a)

5.3 Third data protection principle – adequacy and relevance

> *'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.'*
>
> **DPA 1998**

'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 DPA's third data protection principle is that 'personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed' (DPA, 1998)

Collect only what you need

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 shall be accurate and, where necessary, kept up-to-date.'*
>
> **DPA 1998**

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 processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'*
>
> **DPA 1998**

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 'this principle has close links with both principles 3 and 4. Ensuring personal data is disposed of when no longer needed will reduce the risk that it will become inaccurate, out of date or irrelevant.' (ICO, 2017b)

The NHS Records Management Code of Practice states that clinical audit records should be kept for five years. (IGA, 2016) There is uncertainty as to whether 'clinical audit records' refers to audit reports only or includes the data from which reports are compiled. However, should an audit need to be reviewed, it can be very difficult and time consuming to go back to the data at source, and so it might in any event be prudent to keep the audit data in its collected form.

Ensuring personal data is disposed of when no longer needed reduces the risk that it will become out of date, inaccurate, irrelevant – or a security/data breach risk. When personal data or de-identified data is destroyed, the ICO's guidance on deletion should be followed. (ICO, 2014a)

5.6 Sixth data protection principle – protecting rights of data subjects

> *'Personal data shall be processed in accordance with the rights of data subjects under this Act.'*
>
> **DPA 1998**

The Data Protection Act gives rights to individuals in respect of the personal data that organisations hold about them. These rights include:

- A right of access to a copy of the information included in their personal data
- A right to object to processing that is likely to cause or is causing damage or distress
- A right to prevent processing for direct marketing
- A right to object to decisions being taken by automated means
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
- A right to claim compensation for damages caused by a breach of the Act

Supporting these rights requires transparency, and 'fair processing information' should be given to patients, or made readily available to them. (DPA, 1998) As the name suggests 'fair processing information' is the information needed to make the use of personal data fair. It should state:

- Your organisation's identity and contact details
- That the patient's personal information may be used for quality improvement studies
- A brief explanation of what quality improvement studies are
- The benefits of quality improvement studies
- That information will only be used in identifiable form if it is necessary
- That any identifiable information about them will be protected by strict NHS security measures
- That it will be deleted when it is no longer needed
- That the patient has the right to object
- That the patient has the right to complain

'Fair processing information' is usually given in the form of privacy notices. (ICO, 2016a) The ICO suggests a 'layered' approach by which basic privacy information can refer to 'more detailed information available elsewhere for those who want it'. (DPA 1998) *Appendix 1* of this guide contains a basic template privacy notice, which may be expanded for organisational use.

5.7 Seventh data protection principle – security

> *'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'*
>
> **DPA 1998**

The seventh data protection principle aims to preserve and secure personal data for as long as necessary. (ICO, 2017c) The DPA adds that the level of security should be 'appropriate to the nature of the information in question; and the harm that might result from its improper use or from its accidental loss or destruction.' (DPA, 1998)

Under the DPA, personal data about health is sensitive by definition. Its breach, destruction or improper use is capable of causing serious loss or harm. Healthcare personal data should be protected by the strictest security measures, including during transfer. An organisation and their teams compliant to level 2 of the NHS IG Toolkit should, as data controllers and processors, have such measures in place. However, where there is uncertainty about any aspect of the security of data within quality improvement studies, the advice of an organisational IG lead such as a SIRO or Caldicott Guardian (see *section 1.2* of this guide) should be sought.

The IG Toolkit also contains guidance on handling information security incidents, and procedures for doing so. Organisations should familiarise themselves with such information in case of incident.

5.8 Eighth data protection principle – limited international transfer

> *'Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.'*
>
> **DPA 1998**

With the globalisation of research programmes for quality improvement, growth in big data collection and analysis, and international audits gathering local or regional clinical audit data, care must be taken in sharing data outside of the European Economic Area. Although personal data will not ordinarily need to be shared, should there be a requirement for international transfer, assurance should be sought to ensure that there is adequate protection of the rights of patients with respect to the processing of their personal data within the destination country or countries.

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.

7 Freedom of information and DPA subject access

The *Freedom of Information Act 2000 (FOIA)* covers any recorded information held by a public authority. All NHS organisations are public authorities. Under the FOIA they are obliged to publish certain information about their activities through 'publication schemes' and members of the public are entitled to request information from them.

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)

The FOIA doesn't give people access to their personal data, but requests for such access can be made under the 'subject access' provisions of the DPA. Most personal clinical data is copied from existing data that can be disclosed following a request. The ICO gives helpful guidance on *FOIA publication schemes/requests* and *DPA subject access requests*. (ICO, 2016b and 2017d)

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

Whether your quality improvement study requires the sharing of personal data or de-identified data (because of the risks of re-identification with de-identified data – as opposed to data anonymised for publication), it is good practice to have an information sharing agreement (ICO, 2011) in place, as part of the study protocol. 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

NHS Digital states that 'sharing for direct care can take place across departmental and organisational boundaries. For example, the direct care team may include physiotherapists, nurses, midwives, occupational therapists and others on regulated professional registers'. (NHS Digital, 2013c) There is no obvious reason why 'organisational boundaries' should not include 'boundaries' between primary and secondary care. 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, 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.

Caldicott 2 adds, 'when whole records are shared, patients do not have the ability to block access to individual pieces of information about their care, and this does not align with the principle of sharing only relevant information'. It 'concludes that [explicit] consent should be obtained before sharing a patient's whole care record with other registered and regulated health and social care professionals for the purposes of direct care'. (Department of Health, 2013c)

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 2, 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, 2017) 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

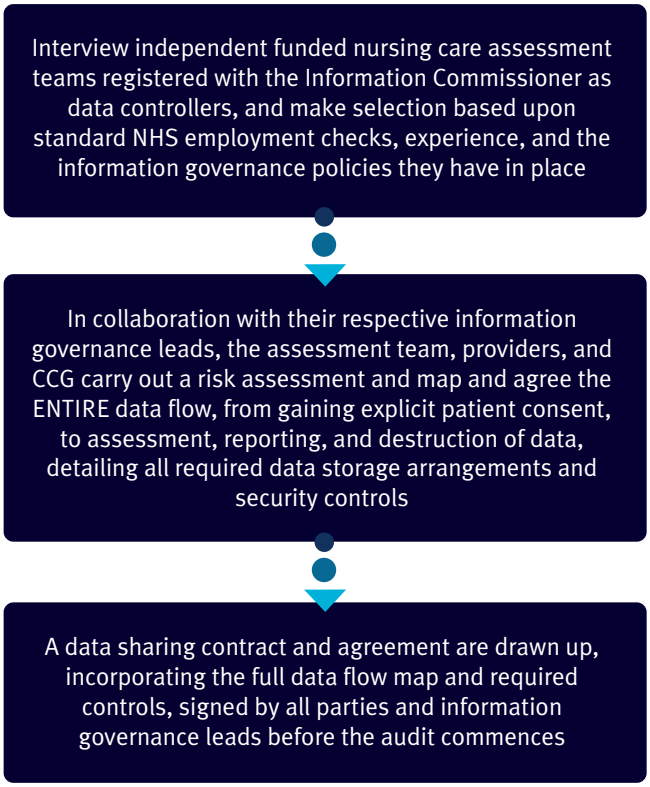
of patients – healthcare quality improvement leads within commissioning organisations might formally examine health records directly, or through an intermediary organisation, with explicit consent from patients and all the necessary controls in place as per the case example and flowchart below.

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.

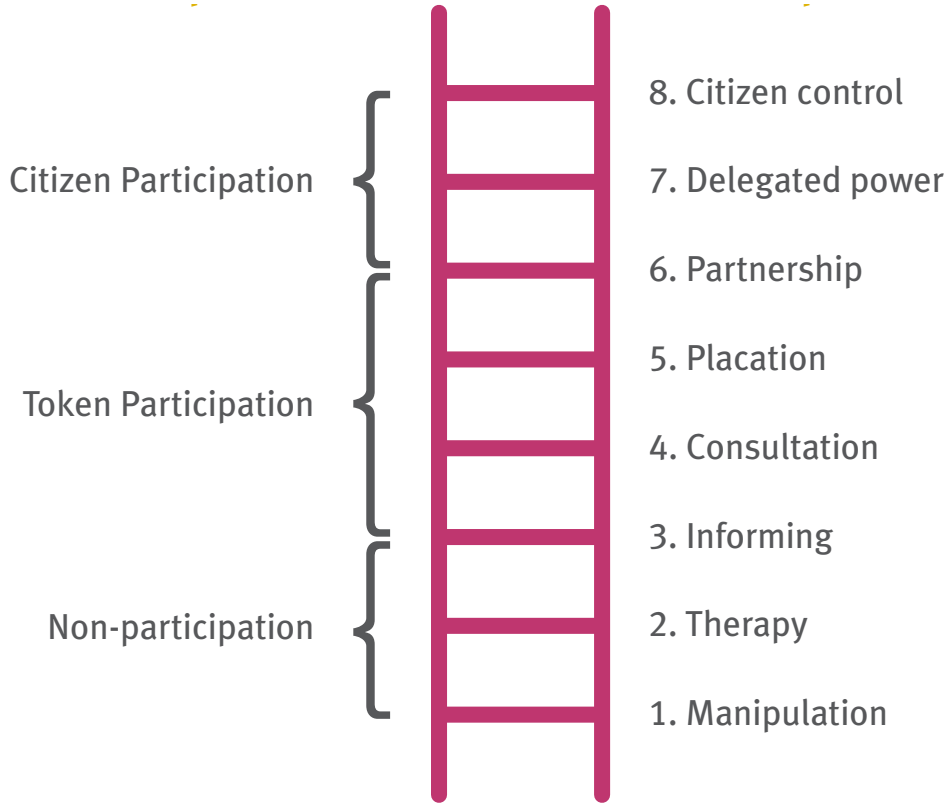


11 Patient and public involvement

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, *Transforming Participation in Health and Care*, (NHS England, 2013b) describes the importance of engaging with patients, carers and the public when redesigning or reconfiguring healthcare services.

The publication references Arnstein's ladder of participation (Arnstein, Sherry R,. 1969) (see below), which places informing the public of services available and the results of quality improvement projects and consultations as low level involvement, with partnership and citizen-led activity at the top of the ladder, stating: 'Patient and public voice activity on every step of the ladder is valuable, although participation becomes more meaningful at the top of the ladder.' (NHS England, 2013b)

> *'Every part of our health and care system is shaped and improved by involving those who use and care about our services. Everyone contributes their distinctive perspective, especially those who face the greatest health disadvantage and the poorest health outcomes. Progressing from listening and understanding, to collaboration and responsiveness, we all benefit from a rich understanding of what is needed and how to co-design and deliver services that meet these needs.'*
>
> **NHS England, 2013b**



Arnstein's ladder of participation (Arnstein, Sherry R., 1969)

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. (IGA, 2015b) The only legal basis for that is explicit consent.

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 16) 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:

- Information Governance Alliance (IGA) for published guidance and an enquiry service specifically tailored for the health and care sector: *www.systems.digital.nhs.uk/infogov/iga*
- 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, 1998.: *www.legislation.gov.uk/ukpga/1998/29/contents*
6. Data Protection Act 1998, Schedule 1, Part I, paragraph 1: *www.legislation.gov.uk/ukpga/1998/29/contents*
7. 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*
8. 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*
9. 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*
10. Department of Health, 2017: IG Toolkit guidance (NHS) section 13-202 at: *www.igt.hscic.gov.uk/*
11. Freedom of Information Act, 2000: *www.legislation.gov.uk/ukpga/2000/36/contents*
12. General Medical Council (GMC), 2009. Confidentiality guidance paragraph 30: *www.gmc-uk.org/static/documents/content/Confidentiality_-_English_1015.pdf*
13. GMC, 2013. Good Medical Practice paragraph 22: *www.gmc-uk.org/static/documents/content/GMP_.pdf*
14. Health and Social Care Act, 2008 (Regulated Activities) Regulations 2010, regulation 10: *www.legislation.gov.uk/ukpga/2008/14/contents*
15. HQIP, 2016a. Patient and public involvement in quality improvement: *www.hqip.org.uk/public/cms/253/625/19/569/Final%20Online%20PPI%20in%20QI.pdf?realName=gdZQ7X.pdf&v=0*

16. HQIP, 2016b. Developing a patient and public involvement panel for quality improvement: www.hqip.org.uk/public/cms/253/625/19/570/Final%20Patient%20Panel%20Guide.pdf?realName=cpDflF.pdf&v=0

17. Human Rights Act 1998: www.legislation.gov.uk/ukpga/1998/42/contents

18. Information Commissioner's Office (ICO), 2011. Data sharing code of practice: www.ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

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

20. 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

21. ICO, 2014a. Deleting personal data: www.ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

22. ICO, 2014b. Conducting privacy impact assessments: www.ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

23. 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

24. ICO, 2016a. Privacy notices code of practice: www.ico.org.uk/about-the-ico/privacy-notices-transparency-and-control/

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

26. ICO, 2017a. The amount of personal data you may hold: www.ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/

27. ICO, 2017b. Retaining personal data: www.ico.org.uk/for-organisations/guide-to-dataprotection/principle-5-retention/

28. ICO, 2017c. Information security. www.ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

29. ICO, 2017d. Subject Access Request: www.ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/

30. ICO, 2017e Data sharing checklists: www.ico.org.uk/media/fororganisations/documents/1067/data_sharing_checklists.pdf

31. IGA, 2015a. Honorary Contracts: IG issues page 2. An example letter of authority is set out in an appendix: www.igt.hscic.gov.uk/Resources/Honorary%20contracts.pdf

32. IGA, 2015b. Honorary contracts: IG issues: www.igt.hscic.gov.uk/Resources/Honorary%20contracts.pdf

33. Information Governance Alliance (IGA), 2016. IGA Records Management: Code of Practice for Health and Social Care: www.digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016

34. NHS Digital, 2017a. Anonymisation Standard for Publishing Health and Social Care Data. ISB 1523: www.content.digital.nhs.uk/isce/publication/isb1523

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

36. National Data Guardian, 2016. Review of data security, consent and opt-outs: www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

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

38. NHS, 2013a. The functions of clinical commissioning groups: www.england.nhs.uk/wp-content/uploads/2013/03/a-functions-ccgs.pdf

39. NHS England, 2017. NHS Standard Contract 2017/18, General Conditions paragraph 15.8: www.england.nhs.uk/wp-content/uploads/2016/11/3-general-conditions-fl-v2.pdf

40. NHS Digital, 2013a. A guide to confidentiality in health and social care: references page 8: www.content.digital.nhs.uk/media/12823/Confidentiality-guide-References/pdf/confidentiality-guide-references.pdf

41. 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

42. NHS Digital, 2013c. A guide to confidentiality in health and social care, page 28: www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

43. NHS Digital, 2015. Patient objections management: www.gov.uk/government/uploads/system/uploads/attachment_data/file/469290/Data-Provision-Notice_Patient_Objections_Management_19.10.15.pdf

44. NHS Digital, 2017. DARS Guidance Notes on Security www.content.digital.nhs.uk/media/15698/DARS---Guidance-Notes-on-Security/pdf/Guidance_Notes_on_Security_v4.0_(1).pdf

Appendix 1 – Patient leaflet/poster and privacy notice template

The following template contains:

- Recommended content for a patient leaflet/poster on the use of personal data for clinical audit and quality improvement
- The information necessary to meet the Data Protection Act requirements for a basic 'fair processing' notice (see main guide section 5.6)
- Information for patients who choose not to have their personal data used for any purposes outside the provision of direct care

The content should be adapted and customised to meet your needs as individual healthcare providers, and where local examples or information should be substituted, content is highlighted with pink text. Healthcare providers should develop their own 'opt out' form and both the form and the final leaflet/poster should be approved by your Caldicott Guardian and Senior Information Risk Officer.

Copies of the leaflet/poster should be freely available to all patients and service users.

The content of this leaflet/poster has been developed with the assistance of members of the HQIP Service User Network (SUN).

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 and the care we provide to you. 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 1-907 561 -25-2

6th Floor, 45 Moorfields, London, EC2Y 9AE

T 020 7997 7370 F 020 7997 7398
E communications@hqip.org.uk

www.hqip.org.uk

Registered Office: 70 Wimpole Street, London W1G 8AX
Registration No. 6498947
Registered Charity Number: 1127049

June 2017. Next review date: June 2018

Information
Governance
Alliance IGA