

# An Information Governance Guide for Clinical Audit

**Wendy Harrison and Heather Sharp**  
**NHS Bradford and Airedale**

*Clinical audit tool to promote quality for better health services*



**Revised - minor changes to  
wording and appendix added -  
November 2011**

**Previous versions:**

September 2009 (first publication)

## Contents

---

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Aims of the guide	1
1.2	What is information governance?	1
1.3	Laws affecting confidential information and their impact on clinical audit	2
<b>2</b>	<b>Informing patients about the use of their information for clinical audit</b>	<b>2</b>
<b>3</b>	<b>Justifying the use of patient information in clinical audit</b>	<b>3</b>
3.1	Topic selection	3
3.2	Interface audit	3
3.3	Your data collection tool	4
3.4	Source of data	4
<b>4</b>	<b>The use of patient identifiable information for clinical audit</b>	<b>4</b>
4.1	What is patient identifiable information in relation to clinical audit	4
<b>5</b>	<b>Access to information for clinical audit</b>	<b>6</b>
5.1	Freedom of Information requests	6
5.2	Data protection Act 1998 – subject access requests	7
<b>6</b>	<b>Transferring clinical audit data</b>	<b>7</b>
6.1	Reporting lost clinical audit data	8
<b>7</b>	<b>Information security</b>	<b>9</b>
7.1	Do's and don'ts for handling information securely	9
7.2	Guidance on how to create a secure password	10
7.3	Guidance on how to protect data by Winzipping and encryption	10
<b>8</b>	<b>Storage and retention of clinical audit data</b>	<b>10</b>
8.1	Guardianship of clinical audit data	10
<b>9</b>	<b>Handling national clinical audit data</b>	<b>11</b>
<b>10</b>	<b>Secondary uses of clinical audit data</b>	<b>11</b>
	<b>References</b>	<b>12</b>
	<b>Appendices</b>	
	Appendix 1. Laws affecting the use of clinical audit information	13
	Appendix 2. Patient identifiable data vs anonymised/pseudonymised data	15
	Appendix 3. Clinical Audit Information Transfer Log	16
	Appendix 4. Guidance on how to encrypt and email data using Winzip 9.0 or above	17
	Appendix 5. Information Governance checklist	19



## 1 Introduction

---

The Healthcare Quality Improvement Partnership (HQIP) is led by a consortium of the Academy of Medical Royal Colleges, the Royal College of Nursing and National Voices. Our purpose is to promote quality in healthcare, and in particular to increase the impact that clinical audit has on healthcare quality in England and Wales.

Clinical audit may be defined as “a quality improvement process that seeks to improve patient care and outcomes through systematic review of care against explicit criteria and the implementation of change. Aspects of the structure, processes, and outcomes of care are selected and systematically evaluated against explicit criteria. Where indicated, changes are implemented at an individual, team, or service level and further monitoring is used to confirm improvement in healthcare delivery”.<sup>1</sup>

In order to facilitate this, HQIP have funded the development of a number of clinical audit support tools to help local teams deliver local clinical audit activity. They are intended to be used as reference material or toolkits to help with the clinical audit process.

This document should be read in conjunction with the following:

- the separate glossary provided
- other relevant tools produced as part of this collection by HQIP.

### 1.1 Aims of the guide

This guide aims to:

- tell you what information governance is all about
- explain areas of the law regarding confidentiality to ensure you are working within them
- inform you of your Information governance responsibilities at each stage of the clinical audit process
- ensure that you know how to handle/store/destroy information appropriately
- give you best practice guidelines
- give you simple do's and don'ts for handling information during the clinical audit cycle
- provide guidance on advising patients about how their information may be used for clinical audit purposes
- take you through an awareness checklist.

### 1.2 What is information governance?

Information governance is a framework for handling personal information in a confidential and secure manner, to appropriate ethical and quality standards, in a modern health service. It sits alongside clinical governance, research and corporate governance and brings together all the requirements, standards and best practice which apply to the handling of personal information. Having robust information governance working practices gives patients/clients confidence that their information will not be disclosed or used inappropriately.

### **1.3 Laws affecting confidential information and their impact on clinical audit**

**All organisations handling personal information have to comply with the acts/laws shown in Appendix 1 (this includes the use of personal information for clinical audit purposes).**

The list in Appendix 1 is not exhaustive and cannot provide authoritative legal advice, but it aims to raise awareness of the laws applying to data sharing/handling, allowing the user to make provisions for the safety of the data at the very start of the clinical audit project. There are also further codes of practice which NHS organisations must follow for example, Department of Health (DH) Confidentiality NHS Code of Practice, the Care Record Guarantee and the Caldicott Principles, all of which govern the use of patient information.

There are six Caldicott principles you must follow when handling patient information:

- Justify the purpose(s) of using confidential information.
- Only use when absolutely necessary.
- Use the minimum that is required.
- Access should be on a strict need-to-know basis.
- Everyone must understand their responsibilities.
- Understand and comply with the law.

The rest of this guide will outline the key aspects of information governance which impact on areas of the clinical audit cycle.

## **2 Informing patients about the use of their information for clinical audit**

---

The General Medical Council states “clinical audit is essential to the provision of good care”. All doctors in clinical practice have a duty to participate in clinical audit. Where an audit is to be undertaken by the team which provided care, or those working to support them, such as clinical audit staff, you may disclose identifiable information, provided you are satisfied that patients are informed about the potential use of their data.

As described in appendix 1, Section 251 of the NHS Act allows patient information to be used for clinical audit without explicit patient consent if data cannot be anonymised. There may be some occasions where although consent is not a requirement it may be good practice, e.g. the involvement of children or mental health topics. If patient leaflets may not be understood by children, best practice would be to ensure that parents, carers or attorneys are able to consent and are aware of how information may be used. Where patients lack mental capacity, the views of family members, carers or an appointed attorney should be sought, although only the patient is able legally to consent.

Although explicit consent is not required patients should be informed about how their information could be used in the NHS including the potential use of their information for clinical audit. In order to assist with this an example patient information leaflet is available. The leaflet aims to help patients understand why we might need to use their information for clinical audit.

**TIP:** Upload from [www.hqip.org.uk](http://www.hqip.org.uk) a copy of the *Using your health records to improve healthcare: Clinical audit in the NHS* leaflet to your website.

If patients decide they would prefer not to have their information used in clinical audit, steps should be taken locally to prevent inclusion in further clinical audit projects e.g. a code added to the electronic record, highlighted on the paper record or a local database of those who have requested not to be included. The decision of patients not to be involved may be based around how their information may be used or shared and they may change their decision if they can be assured that their information will be held securely. For this reason organisations should take steps locally to raise the profile of clinical audit with patients.

### **3 Justifying the use of patient information in clinical audit**

---

#### **3.1 Topic selection**

Clinical audit is a quality improvement activity which does not require direct ethical approval or Caldicott Guardian input. However, it is good practice to consider the following when selecting a clinical audit topic to ensure that patient records are being accessed for justified purposes:

- Has the project been prioritised as part of an annual clinical audit programme? (More guidance is available in *Clinical Audit Programme Guidance Tools* available from HQIP.)
- Has the project been registered through your organisations internal processes for clinical audit?
- Have the key stakeholders been agreed and the project lead or sponsor identified?
- Have all staff involved had appropriate information governance training and do they have confidentiality clauses which have been written into their contracts?

#### **3.2 Interface audit**

You may be carrying out a clinical audit that crosses the interface between different NHS or non-NHS organisations. In these circumstances the general principles in this guide should still be adhered to by all involved to ensure justified and agreed use of the data by all partners. Any local protocols for sharing information between different health and social care organisations should also be followed. To help ensure that there is an agreed justified use of the data by all parties involved, formal 'sign up' to the clinical audit would be advisable. Your organisation may have an overarching information sharing protocol with the organisation you are undertaking the audit with and you should consult your information governance team for advice regarding this. You may also wish to create a record of any data sharing which takes place and an example log is shown in Appendix 3.

**TIP:** To ensure that all parties involved in an interface audit have agreed to the use of relevant data, consider getting the following key individuals from each organisation to sign the clinical audit project registration form:

- lead clinician
- medical director
- Caldicott guardian
- senior information risk owner (SIRO)
- information governance lead.

### 3.3 Your data collection tool

When designing a data collection tool you should ensure you are only collecting the information you require in order to fulfil the aims and objectives of the clinical audit project. Unnecessary information should not be collected/recorded. Do not include the name, address and NHS number of the patient as this is unlikely to be required during the audit.

### 3.4 Source of data

When planning a clinical audit project you should ensure you consider the appropriate source(s) of data. For example, if you are looking in the patient notes will there be any aspects of information within them that you may not need to access to for the audit.

Will you need access to third party information, e.g. GP records/clinical system data? If so, how will you assure the holders of the information that your audit is part of the organisation's clinical audit annual programme?

Are the data available in an anonymised format?

If not, are you able to anonymise/pseudonymise the data?

Think about whether or not you may need to go back over the data, e.g. if there are data quality issues, will you need to be able to identify a particular patient? If so, you will need to pseudonymise the data. If using patient identifiable data, please refer to section 2.

**TIP:** Refer to Appendix 3 for the definitions of identifiable, anonymised and pseudonymised data.

## 4 The use of patient identifiable information for clinical audit

---

### 4.1 What is patient identifiable information in relation to clinical audit — Patient identifiable data vs anonymised data

Historically there has been some misunderstanding around the difference between patient identifiable data and anonymised/pseudonymised information. In general terms patient identifiable data are data that can be directly linked back to a living individual. This can be done directly by including sufficient details such as name, address, sex, date of birth, postcode, phone number, condition, medication etc or by use of a key such as the NHS

number or your own local key. In both cases the data can be linked back to a single living individual. Processing of patient identifiable data is subject to the provisions of the Data Protection Act 1998.

It is a common misconception that data are anonymous if the recipient does not have access to the key. It must be noted that **ANY** data associated with a unique key which refers to a single living individual are patient identifiable data and are subject to the Data Protection Act. Please see Appendix 2 for a detailed key.

**Individual patients should not be directly identifiable throughout the whole clinical audit process** e.g. identifiable from the patient list, electronic database, report and presentation etc.

If this is necessary, then patient consent could be required. Before proceeding you may need to re-think the project plan to confirm that individual patients definitely need to be personally identified throughout the project. Advice should be sought from the Caldicott Guardian if this is still the case after a review of the plan as it would be extremely rare for a clinical audit project to require this. You should also consider that undertaking an audit project with a small number of participants e.g. a rare clinical condition could make individual patients identifiable. In these circumstances additional steps may need to be taken to ensure confidentiality of any small unique groups of patients.

In the majority of clinical audits there may need to be a link from the clinical audit data back to the individual patient record. This link is especially important if the clinical audit results indicate an issue with the provision of care or if data quality issues require patient notes to be re-examined after primary analysis. For this reason in most circumstances clinical audit data will need to be pseudonymised.

If it is not necessary in your clinical audit to have the link back to individual patients from the

**TIP: How to pseudonymise your clinical audit data**

Consider holding a secure file in a different location to the clinical audit data which contains the unique numbers (not NHS number) given to the data collected linked to the patient identifiable items of information. This will allow you to link the data to the patients again should you need to but it will mean that clinical audit data alone will not identify individuals.

clinical audit results e.g. summarised numbers with no potential follow up required, you should ensure that you are not collecting any items of data which could identify individuals. Some possible areas where this may occur include:

- data collection sheets
- patient lists
- spreadsheets/databases for the analysis.

## 5 Access to information for clinical audit

---

When thinking about information governance issues it is important to consider who will require access to the information, what level of access they will require and for how long access will be necessary.

Consider the following groups of people:

- Clinical staff may need access to all data.
- Clinical audit team could require access to all data.
- Administrative staff should only need access to anonymised data.

Ensure that you assess the levels of access for different staff groups in the planning stages and ensure appropriate access controls are in place i.e. only those who need to have access to clinical audit data, should have access. A mechanism for cancelling access also should be in place to ensure that staff who leave the organisation no longer continue to have access. This is especially important in acute settings where medical staff are rotated and may well have started a clinical audit project but are unable to complete it.

Another group to consider are third parties (i.e. drug companies who may provide a sales representative to undertake an audit on a particular group of your patients). You need to ensure that their proposals are ethical, in line with your organisation's clinical audit programme and only give appropriate access to your clinical system if the project has been formally agreed. They also should sign a confidentiality agreement to ensure they are aware of their responsibilities whilst undertaking the audit.

Follow the internal protocols in place to ensure that all medical records are traceable, by being recorded either on a patient administration system or via a password protected log created by your team.

**TIP:** Take steps to ensure that only those who require access to information have it. This may include password protected files and folders stored on shared servers and drives. **For a guide on how to password protect files/folders please refer to section 7, Information Security.**

### 5.1 Freedom of Information requests

The Freedom of Information Act, which was passed in November 2000, gives the general right of access to all types of recorded information held by public organisations. The intention of the Act is to encourage a spirit of openness and transparency in the NHS and the whole public sector.

Patients, carers, clients may request information regarding the results of clinical audits and consideration will need to be taken of how the results will be stored, for how long and how accessible they will be. If results of clinical audits are routinely published and available to the public, then it is sufficient for the requester to be given a link or instructions on where to access the information they have requested. Any information to be released must be checked to ensure there is no link to identify the data subjects or the clinicians involved in the audit.

Before anything sensitive is sent, the local information governance team should be consulted.

Each organisation should also have a dedicated person responsible for managing Freedom of Information requests. This individual should provide guidance on the release of any clinical audit information to the public. For further information, Healthcare Quality Improvement Partnership (HQIP) has specific guidance of the release of clinical audit information following a Freedom of Information request.

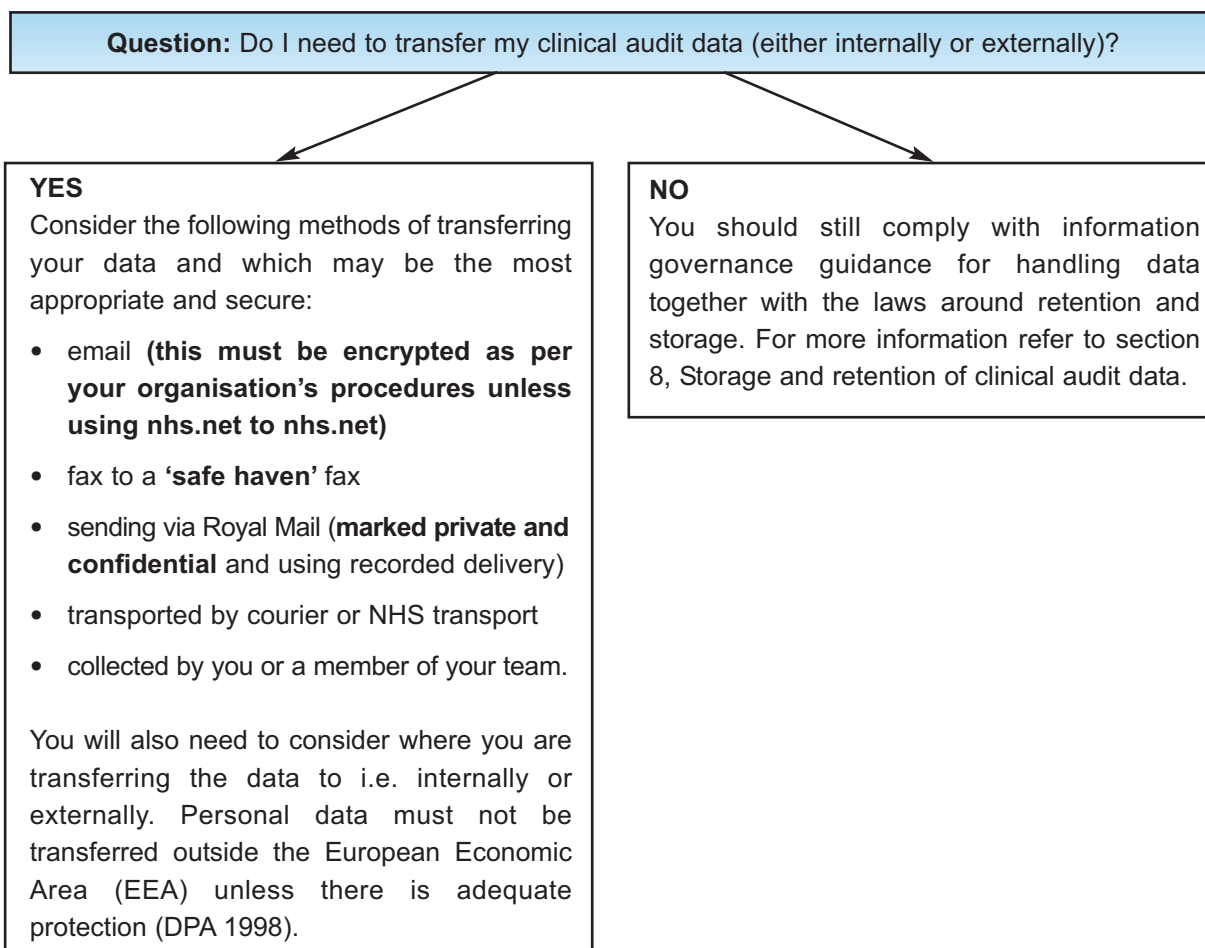
## 5.2 Data Protection Act 1998 – subject access requests

If a patient/client wishes to obtain copies of their own NHS records, this must be requested as a subject access request under the Data Protection Act 1998. Contact your organisation's registered data controller for further information on this process.

## 6 Transferring clinical audit data

---

Data are the key to your clinical audit so ensuring that they can be transferred safely and securely is very important. You may be working collaboratively with other teams either within or outside of your organisation. **It is your responsibility to ensure the safety of data you are using for your clinical audit. You must adhere to your organisation's procedures for secure data handling and seek assurance that the receiving person/team/organisation is aware of their responsibilities to handle and store data securely. You should also seek assurance that clinical audit data will not be given to or be accessible to anyone not involved with the clinical audit project.**



**TIP:** To help ensure information is not lost during transfer you could consider using an information log to record all transfers of clinical audit data. This could be done in a variety of ways but some suggested methods may be:

- ensure there is confirmation of sending and receipt (via email or telephone)
- creation of a spreadsheet or written form to log all activity and data movement (see Appendix 3 for a sample log).

## 6.1 Reporting lost clinical audit data

The Department of Health have categorised loss of identifiable data as shown in the table shown below.

0	1	2	3	4	5
No significant reflection on any individual or body Media interest very unlikely	Damage to an individual's reputation Possible media interest, e.g. celebrity involved	Damage to a team's reputation Some local media interest that may not go public	Damage to a service's reputation/ Low key local media coverage	Damage to an organisation's reputation/ Local media coverage	Damage to NHS reputation/ National media coverage
Minor breach of confidentiality Only a single individual affected	Potentially serious breach Less than 5 people affected or risk assessed as low, e.g. files were encrypted	Serious potential breach and risk assessed high e.g. unencrypted clinical records lost Up to 20 people affected	Serious breach of confidentiality e.g. up to 100 people affected	Serious breach with either particular sensitivity e.g. sexual health details, or up to 1000 people affected	Serious breach with potential for ID theft or over 1000 people affected

If your data are anonymised it does not have to be reported as a Serious Untoward Incident (SUI) but it should be reported as an incident via your organisation's incident reporting mechanism. Whether the information is anonymised or not the risk of any potential harm to patients involved in the clinical audit will need to be assessed and an investigation undertaken to ensure that the risk of any future data loss can be mitigated.

Incidents classified at a severity rating of 3–5 are those which should be captured as Serious Untoward Incidents and should be reported to the Strategic Health Authority (SHA) and the Information Commissioner.

Incidents classified at a severity rating of 0–2 should be included in your organisation's incident reporting procedures and an investigation undertaken to determine the cause and effect of the loss. Please note that information lost or stolen which has been encrypted to NHS standards does not have to be reported as a SUI.

For further information please refer to the Connecting for Health guidance document relating to reporting and managing Serious Untoward Incidents as follows: <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/suichecklist.pdf>

## 7 Information security

---

### 7.1 Do's and don'ts for handling information securely

#### When handling clinical audit information YOU MUST:

##### ALWAYS —

- Protect your team's/network's files and folders by ensuring that permissions are up-to-date and only those who need access have access.
- Seek assurance that those who need access to the clinical audit data are aware of their information governance responsibilities.
- Give passwords/access to those members of staff who need it for the clinical audit.
- Operate a clear desk policy. Lock paper information away when you're not using it.
- Secure your workstation when absent from your desk by activating a password protected screen saver or using Ctrl-Alt-Del-Lock workstation if your network supports this.
- Ensure that databases are password protected, even if the information is anonymised/pseudo-anonymised.
- Encrypt data, so that if information needs to be stored on portable media (i.e. disk, CD, USB) or emailed (either internally or externally) to someone else, you know it is secure.
- Log the retention period for the audit data, so that it can be destroyed when no longer required.
- Destroy clinical audit data in line with your organisation's procedures i.e. in a confidential manner.
- Maintain a log of when clinical audit data was destroyed. (You may need this in the event of a Freedom of Information request.)

##### NEVER —

- Leave patient notes/audit data unattended on your desk.
- Transfer data by any method, without ensuring it is being done so securely.
- Include patient details in your audit proforma unless you have the patient's consent.
- Save information to your local 'C' drive as if your pc fails or is stolen you will lose your data.
- Input information into a database without anonymising/pseudonymising it.
- Create databases without ensuring they are password protected.
- Email audit data without winzipping and encrypting it first.
- Keep data forms, databases etc for longer than necessary.
- Breach legal requirements or be ignorant of the legal requirements that affect you.
- Pass any data used in your audit to anyone who does not have a legitimate right to use the information (i.e. third parties inside or outside of your organisation).

## 7.2 Guidance on how to create a secure password

A secure password should contain a combination of upper and lower case letters, numbers and characters. It should be random and not be able to be easily guessed by those who do not require access to the information.

A good way to create a password is to link it to a phrase i.e. The **diabetes clinical audit takes place in March 09**. Your password would then be **TdcatpiM09** or you could use your current favourite song. **You should always mix your phrases to ensure that the logic behind them is not easily identifiable and your passwords easily guessed.**

## 7.3 Guidance on how to protect data by Winzipping and encryption

Guidance on how to encrypt and email data using Winzip 9.0 or above can be found in Appendix 4 but you must always adhere to your own organisation's procedures for encrypting and transferring information.

# 8 Storage and retention of clinical audit data

---

Clinical audit data should be stored securely throughout the clinical audit process by following the information security guidance in section 7.

You should refer to your organisation's local procedures for retention timescales on clinical audit data collection sheets (proformas) but the Department of Health *Records Management NHS Code of Practice* requires that clinical audit records must be kept securely for a minimum period of 5 years after a clinical audit has been completed. The code does not further define records and therefore you should always follow your own organisation's retention policy regarding the documentation collated or created throughout your clinical audit project. The data should be kept for no longer than the agreed period and should be destroyed confidentially after this time.

## 8.1 Guardianship of clinical audit data

Once your project is complete you may receive requests for copies of clinical audit reports via the Freedom of Information process or from teams who wish to re-audit the topic. You must therefore consider who has guardianship of the information. Create a 'guardian/owner log' of clinical audit projects and clearly show their contact details.

**TIP:** Create a log of all projects facilitated by your team/office/department, which shows who has guardianship of the clinical audit data and reports, their contact details, location of the data, retention period and ultimately when and how it was destroyed. Ensure that contact details are updated when guardians leave or if the clinical audit data is removed to another site. Your organisation may have a central register for clinical audit projects, which should incorporate these details.

All data in whatever format it has been created in relating to the clinical audit project should be stored securely using the guidance tables below:

Storing paper data and information	Storing electronic data and information
<p>Records must be contained within a robust folder which clearly identifies the organisation.</p> <p>Always store in either locked cupboards or rooms and ensure access is appropriate.</p> <p>Bear in mind any environmental hazards, i.e. water pipes which could burst and ruin your data.</p> <p>It is best practice to create a “front sheet” which can be placed on the front of paper files giving information on when the information was created, who is the responsible owner and team of the information and when it should be destroyed.</p> <p>Keep a log of clinical audit projects and their guardian/owner.</p>	<p>Password protect files/folders and only give access to those who need access.</p> <p>If clinical audits are logged on a database information should be added to this to flag up when the data should be destroyed.</p> <p>If not, a log should be created to ensure that the clinical audit team can easily identify when data should be destroyed.</p> <p>It is best practice to create a front sheet which should be easily identifiable when the folder is accessed.</p> <p>Good housekeeping of network folders will ensure that electronic folders are deleted in accordance with your retention period.</p>

## 9 Handling national clinical audit data

---

Information for national clinical audits should be managed by following the guidance provided in this document with regards to access, storage and retention. However, specific national audit bodies may have their own information governance specifications, e.g. registration forms may require sign off from the organisation’s Caldicott Guardian. **Your Caldicott Guardian should always be given details of any national clinical audits your organisation is taking part in. Seek assurance that any data you submit will not be used for any other purpose or transferred to a third party. National audit data should be submitted via the https website.**

For further information about the processes for individual national audits including their information governance requirements please visit the [www.hqip.org.uk](http://www.hqip.org.uk) website.

## 10 Secondary uses of clinical audit data

---

Patient information should not be used for any other purpose than that for which you have collected it. Although you may want to use the summarised, anonymised clinical audit results to support other quality improvement work, you must not give or allow anyone access to the raw clinical audit data without checking whether the team/individual has a legitimate right to access it.

**This includes you; you cannot use the raw clinical audit data you have collected for other projects and especially NOT for research purposes.**

**Healthcare purposes is defined as** all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided.

**They do not include research, teaching, financial audit and other management activities.**

## References

---

1. National Institute for Clinical Excellence. *Principles of Best Practice in Clinical Audit*. Abingdon: Radcliffe Medical Press; 2002.
2. Department of Health. *Confidentiality NHS Code of Practice*. London: Department of Health; November 2003.

## **Appendix 1. Laws affecting the use of clinical audit information (All Acts included in this guide can be viewed on the Office of Public Sector Information website, [www.opsi.gov.uk](http://www.opsi.gov.uk).)**

---

**Data Protection Act 1998** — An Act to make provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. All data subjects have a right of access to their health records, therefore all records should be traceable whilst in your care.

**Always bear in mind that the eight Data Protection Act principles require that personal data must:**

- be processed fairly and lawfully
- be obtained or processed for specific lawful purposes
- be adequate, relevant and not excessive
- be accurate and kept up to date
- not be kept for longer than necessary
- be processed in accordance with rights of data subjects
- be kept secure
- not be transferred outside the European Economic Area (EEA) unless there is adequate protection.

**Freedom of Information Act 2000** — An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them. You may need to respond to requests for information regarding clinical audit projects. Under the terms of the Freedom of Information Act, **anyone** is entitled to apply for copies of clinical audit reports. You should therefore ensure that when reporting clinical audit results, there is no stated link between audit conclusions and patients/clients or clinicians. Presentation of audit results should always have the approval of stakeholders.

**Access to Health Records 1990** — This Act has been superseded by the Data Protection Act but still applies to access to the records of the deceased. An Act to establish a right of access to health records by the individuals to whom they relate and other persons; to provide for the correction of inaccurate health records and for the avoidance of certain contractual obligations; and for connected purposes.

**Human Rights Act 1998** — An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights. The Human Rights Act requires that any invasion of an individual's private life is first subject to a test of necessity and proportionality. It is also underpinned by the Data Protection Act 1998.

**Computer Misuse Act 1990** — An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

**Criminal Justice and Immigration Act 2008** — The Secretary of State may by order provide for a person who is guilty of an offence under section 55 of the Data Protection Act 1998 (c. 29) (unlawful obtaining etc. of personal data) to be liable.

**If you use, obtain or disclose information recklessly and in contravention of the Data Protection Act 1998 YOU may receive a fine or prison sentence of up to two years if you are successfully prosecuted under this Act.**

**Section 251 of the NHS Act 2006** — Section 251 of the NHS Act 2006 re-enacted Section 60 of the Health and Social Care Act 2001. The terms Section 60 and Section 251, when used in relation to use of patient information, therefore refer to the same powers. These powers allow the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for medical purposes where it is not possible to use anonymised information and where seeking individual consent is not practicable.

It was anticipated when section 251 powers were originally established that the NHS would develop mechanisms to seek, record and implement consent. Also that the NHS would endeavour to improve data quality and develop processes to link data in pseudonymised form, reducing the need for identifiable data to be used. These mechanisms are still being developed. The Health Service (Control of Patient Information) Regulations 2002 (SI 1438) were made under Section 60 of the Health & Social Care Act 2001 and continue to have effect under Section 251 of the NHS Act 2006. These regulations established class support mechanisms which support the use of information, one of which allows the use of patient information **under strict controls**, 'for the audit, monitoring and analysing the provision made by the health service for patient care and treatment'.

**Common Law Duty of Confidentiality** — The Common Law Duty of Confidentiality is not an act but is a key issue in matters of sharing or using personal and/or sensitive information. For NHS purposes using personal information can be justified where the recipient needs the information because he or she is or may be concerned with the patient's care or treatment; the use of the information can also be justified for wider purposes such as improving quality of treatment, promoting effective healthcare administration or research. Where information is shared, there is an implied understanding that the information will not be used except where it is strictly needed to help the professional provide the service. Each member of the team, and any person who provides administrative or secretarial support, has an obligation to treat the information as confidential. The obligation of confidence owed by a professional covers not only information provided by the patient, but also information relating to the patient which the professional obtains from others.

## Appendix 2. Patient identifiable data vs. pseudonymised/anonymised data

<b>Patient identifiable information<sup>2</sup></b>	Key identifiable information includes: <ul style="list-style-type: none"><li>• patient's name, address, full postcode, date of birth</li><li>• pictures, photographs, videos, audiotapes or other images of patients</li><li>• NHS number and local patient identifiable codes</li><li>• anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.</li></ul>
<b>Pseudonymised information</b>	This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.
<b>Anonymised Information</b>	This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification. As above, care must be taken where small numbers of anonymised data recorded against rare conditions could identify patients in a demographic area.

### Appendix 3. Clinical Audit Information Transfer Log

#### CLINICAL AUDIT INFORMATION TRANSFER LOG

Complete this form to log all transfers of information which take place during a clinical audit project (electronic and hard copy). This will ensure all information is tracked and anonymising data can be flagged up.

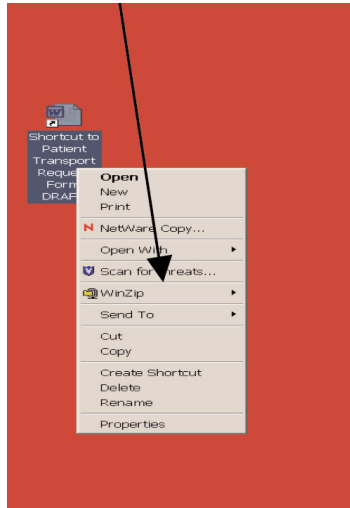
Clinical Audit Project Title	Information being transferred	Controlled/identifiable information (Y/N) whether pseudonymised	Form of information being transferred	Method of encryption/level of security	Personnel	Date ticked or passed on to recipient	Date of expected receipt	Date of receipt	Method of receipt
EXAMPLE 1: Diabetes audit	Collected data ready for analysis	N	Excel file	Email	Pass word protected and encrypted	Planned	3/1/08	3/1/08	Planned
EXAMPLE 2: Falls audit	Data collection forms	Y	Paper copy	Computer	Computer signature required on receipt, masked private and confidential	Awaiting receipt	3/1/08	3/1/08	Awaiting receipt

## Appendix 4. Guidance on how to encrypt and email data using Winzip

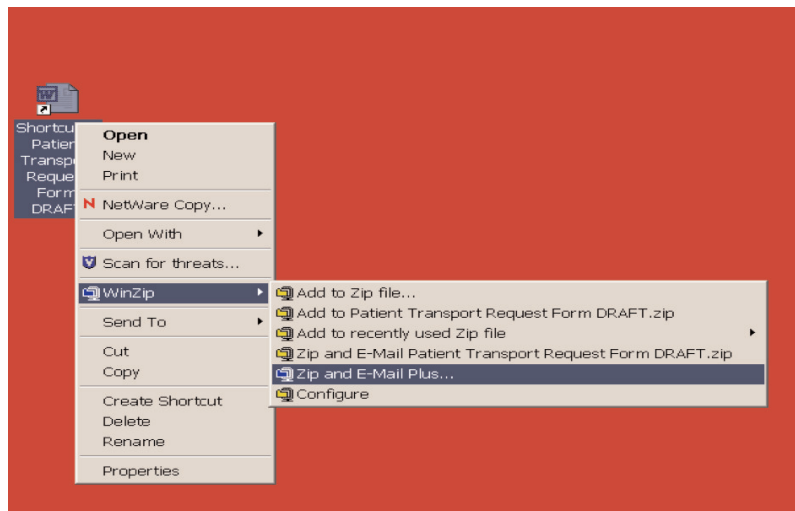
---

Please note: the following examples may look different depending on which version of Winzip is being used.

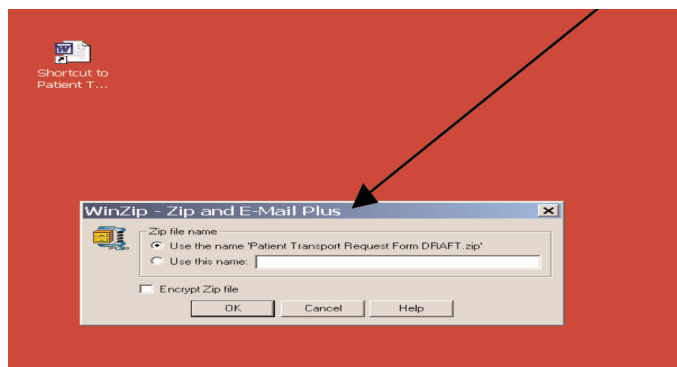
Find the location of the saved document you wish to send via email and then right mouse click to bring up the options box as shown below:



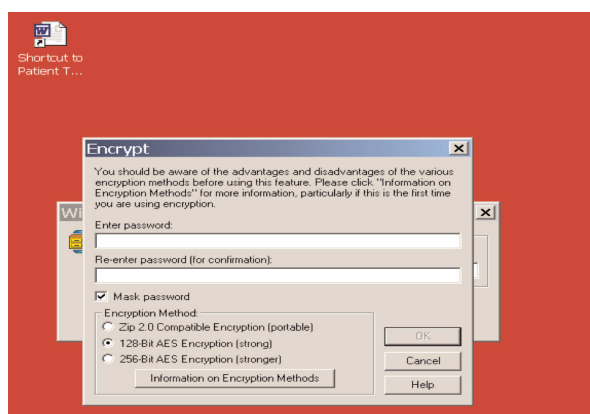
Click on the Winzip and choose zip and email plus.



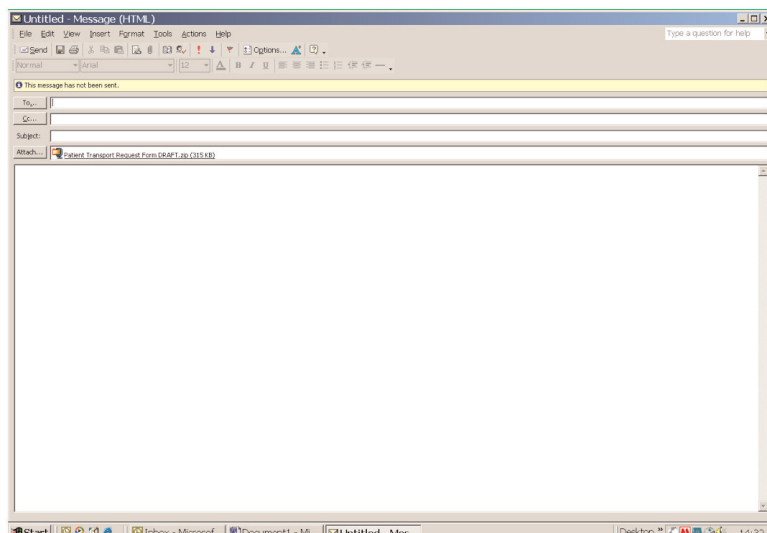
You are then given the following options and you need to click in the Encrypt zip file as shown below and press ok.



You will then be asked to create and confirm a password, AES 128 or better AES 256 should always be used when encrypting a file.



'Once you have chosen your secure password and pressed OK, the document uploads into an email ready to send. For guidance on how to create a secure password see 7.2. Always ensure that you send your password in a separate email or telephone it through to the recipient.'



If you need to encrypt data to store it onto removable media such as a USB memory stick or CD, choose “add to zip file” rather than zip and email plus. This will allow you to create an encrypted file which you can then transfer to your USB or CD.

NHS Connecting for Health has completed the national procurement of an encryption solution for removable media and full disk encryption on behalf of the NHS. For all the latest information relating to this NHS encryption tool initiative, please visit the encryption tool section. Any further queries can be directed to [cfh.encryptedtool@nhs.net](mailto:cfh.encryptedtool@nhs.net).

## Appendix 5. Information governance checklist

---

Before beginning your clinical audit ensure you have considered all of the following areas:

- Have you registered your clinical audit project with your organisation's clinical audit team?
- Will you be using patient identifiable information throughout your audit? (If yes, you may need patient consent and/or the approval the approval of your Caldicott Guardian/ information governance lead.)
- Will you need to anonymise or pseudonymise your data?
- Are clinical audit patient information leaflets generally available in your organisation?
- Are those who have access to the data aware of their IG responsibilities?
- Have you considered any ethical issues (third party access)?
- Who has access to the clinical audit data and at what level (identifiable or anonymised)?
- How will you securely transfer any clinical audit data?
- Have you considered creating a log of any transfers of information which will be happening throughout the project?
- Where will you store the clinical audit data, is this a secure area?
- What is the level of security on any electronic/paper records of your clinical audit data?
- Have you created a password to protect any electronic data?
- Have you informed those staff who need access to the data what the password is?
- Who will be the named guardian/owner of the clinical audit data?
- Have you created a log of clinical audit projects containing the 'guardian/owner' of the data?
- Have you identified the retention period and destruction date for the data?
- Are you using any of the other clinical audit tools available from HQIP?

## Appendix 6. Information Governance Guides

---

NHS Connecting for Health Information Governance

<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov>

The NHS Confidentiality Code of Practice

[http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH\\_4100550](http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550)

Information Security Management: NHS Code of Practice

[http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_074142](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_074142)

Records management: NHS code of practice

[http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_4131747](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747)

The Caldicott Guardian Manual

[http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH\\_4100563](http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100563)

National Information Governance Board for Health and Social Care (NIGB)

<http://www.nigb.nhs.uk/>

Information Commissioner's Office (ICO)

<http://www.ico.gov.uk/>