Confidentiality Policy

NHS England and NHS Improvement

NHS England and NHS Improvement INFORMATION READER BOX		
Directorate		
Medical	Operations and Information	Specialised Commissioning
Nursing	**Trans. & Corp. Dev.**	Strategy & Innovation
Finance		

Publications Gateway Reference:	
Document Purpose	Policy
Document Name	Confidentiality Policy
Author	Corporate Information Governance
Publication Date	September 2019
Target Audience	All NHS England and NHS Improvement Employees
Description	Policy and high-level procedures for Confidentiality
Cross Reference	N/A
Superseded Docs (if applicable)	Confidentiality Policy v5.0
Action Required	To note
Timing / Deadlines (if applicable)	**N/A**
Contact Details for further information	Carol Mitchell Head of Corporate Information Governance Quarry House Leeds LS2 7UE England.ig-corporate@nhs.net

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Confidentiality Policy

Version number: v5.1

Updated: September 2019

Prepared by: Corporate Information Governance

Classification: OFFICIAL

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact England.ig-corporate@nhs.net

Contents

1 Introduction

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within NHS England and NHS Improvement and have access to person-identifiable information or confidential information (see appendix D). All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation – the European General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA2018) which implements the GDPR in the UK.

Confidentiality is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

NHS England and NHS Improvement are cooperating to establish a joint enterprise. This mirrors the focus of the NHS Long Term Plan on how we will deliver integrated care to patients at the local level, how we set the whole of the NHS up to do that and how it will benefit patients and communities. To ensure that we comply with our data protection obligations the three statutory organisations (NHS England and NHS Improvement – which comprises Monitor and TDA) have entered into a Joint Controller and Information Sharing Framework Agreement. This sets out our joint data protection responsibilities and the measures that we have put in place to ensure that we comply. The Information Sharing Policy sets our framework for processing personal data in support of joint working with reference to this agreement.

It is important that NHS England and NHS Improvement protect and safeguard person-identifiable and confidential business information that it gathers, creates processes and discloses, in order to comply with the law, relevant NHS mandatory requirements and to provide assurance to patients and the public.

This policy sets out the requirements placed on all staff when sharing information within the NHS and between NHS and non-NHS organisations.

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted as per current NHS Encryption Guidance or a business case has been approved by the Transformation & Corporate Development Directorate's Information Governance Team.

Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records,

occupational health records, etc. It also includes NHS England and NHS Improvement confidential business information.

Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

A summary of Confidentiality Do's and Don'ts can be found at Appendix A.

The Legal and NHS Mandated Framework for confidentiality which forms the key guiding principles of this policy can be found in Appendix B.

How to report a breach of this policy and what should be reported can be found in Appendix C.

Definitions of confidential information can be found in Appendix D.

2 Scope

All our staff and of hosted organisations, without exception, are within the scope of this policy, including and without limitation:

- Central and Regional Teams;
- All Commissioning Support Units;
- NHS Interim and Management Support (NHS IMAS);
- NHS Sustainable Development Unit;
- Strategic Clinical Networks;
- Clinical Senates; and
- Healthcare Safety Investigation Branch (HSIB)

3 Roles and Responsibilities

3.1 The Chief Executive

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that NHS England and NHS Improvement policies comply with all legal, statutory and good practice guidance requirements.

3.2 The Caldicott Guardian

A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing by providing advice to professionals and staff.

3.3 Senior Information Risk Owner

Sign off and take accountability for risk-based decisions and reviews in regards to the use, disclosure or processing of confidential data in regard to the operating functions of NHS England and NHS Improvement. The SIRO (or their deputy) chairs the National IG Steering Group (see 3.5).

3.4 Data Protection Officer (DPO)

To provide advice to the highest level of the organisation and all of its employees on data protection issues which can include confidentiality issues which would be reviewed in collaboration with the Caldicott Guardian as appropriate to ensure the organisation's compliance with data protection law

3.5 The National Information Governance Steering Group

The National Information Governance Steering Group oversees the development and implementation of Information Governance in NHS England and NHS Improvement and ensures that the organisation complies with supporting the Legal and NHS Mandatory Framework with regard to Information Governance.

3.6 Director with responsibility for HR

The Director with responsibility for HR is responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in corporate inductions for all staff.

3.7 Senior Managers

Senior Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via the Information Security Incident Reporting Procedure.

3.8 Head of Corporate Information Governance

The Head of Corporate Information Governance is responsible for ensuring the policy is kept up to date, providing advice on request to any member of staff on the issues covered within it, and ensuring that training is provided for all staff groups to further their understanding of the principles and their application.

3.9 All staff

Confidentiality is an obligation for all staff. Staff should note that they are bound by the Confidentiality: NHS Code of Practice 2003. There is a Confidentiality clause in their contract and it is mandatory to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues.

Any breach of confidentiality, inappropriate use of health data, staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract, and must be reported to an appropriate line manager and via the NHS England Information Security Incident Portal..

Section 170 (1) of the Data Protection Act 2018: Unlawful obtaining etc of personal data, states it is an offence for a person knowingly or recklessly:

(a) to obtain or disclose personal data without the consent of the controller
(b) to procure the disclosure of personal data to another person without the consent of the controller, or
(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

4 Corporate Level Procedures

4.1 Principles

All staff must ensure that the following principles are adhered to:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with either your Line Manager or the Corporate Information Governance Team.

NHS England and NHS Improvement is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

Person-identifiable information, wherever appropriate, in line with the data protection principles stated in the Data Protection Policy, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data in line with the ICO's Anonymisation Code of Practice.

Access to rooms and offices where terminals are present, or person-identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

All staff should clear their desks at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts and fax messages must not be left lying around but be filed and locked away when not in use.

NHS England and NHS Improvement's Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

4.2 Disclosing Personal/Confidential Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice (https://ico.org.uk/).

- When the information is required by law or under a court order. In this situation staff must raise in the first place with the Corporate IG team by e-mailing the DPO inbox. The IG team will then consult the DPO or Caldicott Guardian if necessary before advising.

- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of patient information) Regulations 2002, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority[1]. Referred to as approval under s251 of the NHS Act 2006.

[1] This group has replaced the NIGB's Ethics and Confidentiality Advisory Group

- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must raise in the first place with the Corporate IG team by e-mailing the DPO inbox. The IG team will then consult the DPO or Caldicott Guardian if necessary before advising.

- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must raise in the first place with the Corporate IG team by e-mailing the DPO inbox. The IG team will then consult the DPO or Caldicott Guardian if necessary before advising.

- For any proposed routine disclosures of personal/confidential information, please consult the IG Requirements for New Processes Procedureto see if a Data Protection Impact Assessment should be undertaken.

If staff have any concerns about disclosing information they must raise in the first place with the Corporate IG team by e-mailing the DPO inbox. The IG team will then consult the DPO or Caldicott Guardian if necessary before advising.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. Data sharing agreements provide a way to formalise arrangements between organisations. For further information on Data Sharing Agreements contact the Corporate Information Governance team or see the Information Sharing Policy.

Staff must ensure that appropriate standards and safeguards are in place to protect against inappropriate disclosures of confidential personal data. See the Safe Haven Procedure for guidance on the safe transfer of confidential or person-identifiable information.

When transferring patient information or other confidential information by email, services or methods that meet NHS Encryption standards must be used. Emails between NHS Mail accounts meet this requirement (nhs.net to nhs.net). Emails between NHS Mail and other secure government domains also meet this requirement (e.g. gov.uk). As there are a number of these, please consult the Corporate IG team for advice when intending to send confidential information by email to a non-nhs.net address.

It is not permitted to include confidential or sensitive information in the body of an email. When e-mailing to addresses other than the secure domains described above the information must be sent as an encrypted attachment with a strong password communicated through a different channel or agreed in advance. When communicating via the secure domains, to protect against the risk of accidentally sending to an incorrect recipient, the data should be sent in a password protected attachment, again with the password communicated through a different channel or agreed in advance.

Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent, or the information is not person-identifiable or confidential information.

4.3 Working Away from the Office Environment

There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry NHS England or NHS Improvement information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents. Please refer to the Mobile Working Procedure.

Taking home/removing paper documents that contain person-identifiable or confidential information from NHS England or NHS Improvement premises is discouraged.

To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations.

When working away from NHS England or NHS Improvement locations staff must ensure that their working practice complies with NHS England and NHS Improvement's policies and procedures. Any electronic removable media must be encrypted as per the current NHS Encryption Guidance.

Staff must minimise the amount of person-identifiable information that is taken away from NHS England or NHS Improvement premises.

If staff need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of NHS England or NHS Improvement buildings.

- Confidential information is kept out of sight whilst being transported.

If staff need to take person-identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information. It is particularly important that confidential information in any form is not left unattended at any time, for example in a car.

Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person-identifiable or confidential information on a privately-owned computer or device.

4.4 Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended.

Steps must be taken to ensure physical safety and security of person-identifiable or business confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is gross misconduct which may result in your summary dismissal. This could also constitute an offence under the Computer Misuse Act 1990.

4.5 Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information about themselves without a legitimate purpose, unless through established self-service mechanisms where such access is permitted (e.g. viewing your ESR record). Under no circumstances should employees access records about their own family, friends or other persons without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and may be an offence under the Data Protection Act 2018.

When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of NHS England and NHS Improvement.

If staff have concerns about this issue they should discuss it with their Line Manager, Corporate Information Governance Team or DPO.

4.6 Confidentiality Audits

Good practice requires that all organisations that handle person-identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by the Transformation and Corporate Development Directorate, Corporate Information Governance team through a programme of audits.

5 Distribution and Implementation

5.1 Distribution Plan

This document will be made available to all staff via the intranet site. A notice will be issued in the staff bulletin notifying of the release of this document.

5.2 Training Plan

The IG Training Programme incorporates a training needs analysis for all NHS England and NHS Improvement staff.

Based on the findings of that analysis, appropriate training will be provided to staff as necessary.

Guidance will be provided on the Transformation and Corporate Development Directorate intranet site.

6 Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Corporate Information Governance team and may be subject to external audit.

The Head of Corporate Information Governance is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

7 Equality Impact Assessment

This document forms part of NHS England and NHS Improvement's commitment to create a positive culture of respect for all staff and service users. The intention is to

identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this document and its impact on equality has been analysed and no detriment identified.

8 Associated Documents

The following documents will provide additional information:

- Acceptable Use of ICT and User Obligations
- Confidentiality Policy
- Corporate Document and Records Management Policy
- Data Protection Policy
- Freedom of Information Policy
- Information Governance Policy
- Information Security Policy
- Information Sharing Policy

Appendix A: Confidentiality Do's and Don'ts

Do's

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of NHS England or NHS Improvement.

- Do clear your desk at the end of each day, keeping all non-digital records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.

- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.

- Do ensure that you cannot be overheard when discussing confidential matters.

- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.

- Do share only the minimum information necessary.

- Do transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gov.uk. For up to date information of secure domains please contact the Corporate IG Team.

- Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent and record the decision and any action taken.

- Do report any actual or suspected breaches of confidentiality.

- Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don’ts

- Don’t share passwords or leave them lying around for others to see.
- Don’t share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don’t use person-identifiable information unless absolutely necessary, anonymise the information where possible.
- Don’t collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix B: Summary of Legal and NHS Mandated Frameworks

NHS England and NHS Improvement is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of NHS England and NHS Improvement, who may be held personally accountable for any breaches of information security for which they may be held responsible. NHS England and NHS Improvement shall comply with the following legislation and guidance as appropriate:

The **European Data Protection Regulation (GDPR) and Data Protection Act (2018)** regulate the use of "personal data" and sets out eight principles to ensure that personal data is:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and where necessary kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Caldicott Report (1997) and subsequent Caldicott or National Data Guardian reviews recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information.
- Don't use patient identifiable information unless it is absolutely necessary.
- Use the minimum necessary patient-identifiable information.
- Access to patient-identifiable information should be on a strict need to know basis.
- Everyone should be aware of their responsibilities.

- Understand and comply with the law.
- **The duty to share information can be as important as the duty to protect patient confidentiality.**

https://www.gov.uk/government/publications/the-information-governance-review

https://www.gov.uk/government/publications/caldicott-information-governance-review-department-of-health-response

Article 8 of the **Human Rights Act (1998)** refers to an individual's "*right to respect for their private and family life, for their home and for their correspondence"*. This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

Click here for an online link to the Human Rights Act 1998

The **Computer Misuse Act (1990)** makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access to data or programs held on a computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.

2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.

3. Unauthorised acts with intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

a. Making, supplying or obtaining articles for use in offences 1-3

Click here for an online link to the Computer Misuse Act 1990

The **NHS Confidentiality Code of Practice (2003)** outlines four main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information.
- Inform patients of how their information is used.
- Allow patients to decide whether their information can be shared.
- Look for improved ways to protect, inform and provide choice to patients.

Click here for an online link to NHS Confidentiality Code of Practice 2003

Common Law Duty of Confidentiality

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law

Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is “ultra vires”, i.e. beyond its lawful powers.

The NHS Care Record Guarantee

The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients’ rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant are:

Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:

- You ask us to do so.
- We ask, and you give us specific permission.
- We have to do this by law.
- We have special permission for health or research purposes; or
- We have special permission because the public good is thought to be of greater importance than your confidentiality, and
- If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of Practice and other national guidelines on best practice.
-

Commitment 9 - We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.

Click here for an online link to NHS Care Record Guarantee

Appendix C: Reporting of Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported to the Corporate Information Governance Team, Transformation and Corporate Development Directorate for NHS. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager or Corporate Information Governance staff. The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to NHS England or NHS Improvement systems either by staff or a third party.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act and NHS Code of Confidentiality.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in a public area.
- Theft or loss of person-identifiable or confidential information.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing of person-identifiable information in an ordinary waste paper bin.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager or Corporate Information Governance staff should be sought.

Reporting of Breaches

A regular report on breaches of confidentiality of person-identifiable or confidential information shall be presented to the National Information Governance Steering Group and the Central Team Information Governance Operational Group . The information will enable the monitoring of compliance and improvements to be made to the policy and procedures.

Appendix D: Definitions

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Special categories of personal information (previously known as 'sensitive' personal data) as defined by the Data Protection Act 2018 refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sexual history and/or sexual orientation
- Criminal data

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.

Version control tracker

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
1.0	April 2013	Information Governance Senior Manager	Approved	New policy
2.0	June 2014	Information Governance Senior Manager		Updated to reflect change of Policy directorate to Transformation & Corporate Operations directorate
2.1	March 2016	Corporate Head of Information Governance	Draft	Updated to include new guidance from ICO and Caldicott 2/NDG review.
3.0	June 2016	Corporate Head of Information Governance	Approved	Yearly review
4.0	August 2018	Data Protection Officer		Updated to reflect new data protection legislation
5.0	March 2019	Information Governance Manager (NHSI)		Alignment with NHS Improvement
5.1	September 2019	IG Manager and Senior Corporate IG Lead	Approved	Amendments to reflect joint working and advice from Counsel