Health Research Authority

Confidentiality Policy

Author:	Deputy Chief Executive and Director of Finance
Date of Release:	November 2020
Version No, Status & Date:	V3.2 FINAL 2023.01.24
Approved By:	Information Governance Steering Group
Supersedes Version:	V3.1
Review Date:	January 2025
Owner:	Deputy Chief Executive and Director of Finance
Scope of Document:	All HRA Staff

Contents

Abbreviations

DPA	Data Processing Agreement

DPA 2018	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO/DDPO	Data Protection Officer/Deputy Data Protection Officer
DSA	Data Sharing Agreement
DSSR	Data Subject Rights Request
ESR	Electronic Staff Record
FOI/FOIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
HRA	Health Research Authority
IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
IT	Information Technology
SIRO	Senior Information Risk Owner
IP	Intellectual Property
PIN	Public Involvement Network
REC	Research Ethics Committee
NREAP	National Research and Ethics Advisors' Panel
EOL	Exchange Online
CAG	Confidentiality Advisory Group

Glossary

Confidential information	Confidential information includes, but is not limited to, all information of a confidential nature relating to the business and affairs of the organisation, its' clients (including research organisations) and employees / contractors / volunteers. A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence.
Freedom of Information Act 2000 (FOI)	The Freedom of Information Act 2000 provides public access to information held by public authorities
Data Protection Act 2018 / UK General Data Protection Regulation	The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is: used fairly, lawfully and transparently.'
HRA Community	Research Ethics Committee members, Confidentiality Advisory Group members and Public Involvement Network members
HRA Staff	'HRA Staff' include directly employed staff, secondees, agency workers, contractors
Information Assets	Includes operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, process and procedures, personal information content, other information content, people skills and experience
Mobile Devices	This includes but is not limited to portable computers such as laptops, notebooks, tablets, mobile telephones, and smart phones
Person Identifiable Information / Data	Key identifiable information includes: Name, address, full postcode, date of birth • Pictures, photographs, videos, audio-tapes or other images (including digital) • Anything else that may be used to identify someone directly or indirectly. For example, rare diseases, drug treatments or statistical analysis which identify small numbers within a small population may allow individuals to be identified.
Data Subject Rights Request (DSSR)	A DSSR is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under the Data Protection Act.

1. Purpose

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

All employees working in the HRA 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 Data Protection Act 2018 (DPA 2018) which implements the GDPR in the UK.

It is important the HRA protects and safeguards 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 with the NHS and with other 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.

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, employee records, occupational health records, etc. It also includes the Health Research Authority's confidential business information.

Information can relate to staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, computer file or printout, laptops, 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.

2. Scope

This policy covers directly employed staff, secondees, agency worker and contractors. The principles of this policy apply to HRA Community members including volunteers from Research Ethics Committees (REC) and the Confidentiality Advisory Group (CAG) and also Public Involvement Network Members. Information Governance principles and requirements for these individuals are covered within terms and conditions / codes of conducts.

This policy applies to all information processed including:

- Manual records such as paper.
- Electronic records such as computer and cloud records and telephone recordings.
- Any extracts taken, printed, copied, transferred or verbally connected with the activities of the HRA.

3. Roles and Responsibilities

3.1 The Chief Executive
The Chief Executive has overall responsibility for strategic and operational management, including ensuring that the HRA 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 The Senior Information Risk Owner (SIRO)
The SIRO is responsible for signing off and taking accountability for risk-based decisions and reviews regarding the use, disclosure or processing of confidential data which relate to the operating functions of the HRA.

3.4 The Data Protection Officer (DPO)
The DPO will provide advice to the highest level of the organisation and all of its employees on data protection issues, which can include confidentiality issues. These issues will be reviewed in collaboration with the Caldicott Guardian as appropriate to ensure the organisation's compliance with data protection law.

3.5 All staff
Confidentiality is an obligation for all staff and a confidentiality clause is included in all staff employment contracts. Everyone working for the HRA who records, handles, stores or comes across information that could identify an individual has a Common Law Duty of Confidence to that individual and to the HRA.

It is mandatory for all staff to participate in induction, training and awareness raising sessions carried out to inform and update staff on information governance and confidentiality issues.

Any breach of confidentiality, inappropriate use of personal 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 Health Research Authority Atlas.

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. What is Confidential Information?

Confidential information includes, but is not limited to, all information of a confidential nature relating to the business and affairs of the organisation, its' clients (including research organisations) and employees / contractors / volunteers. A duty of confidence arises when one person discloses

information to another in circumstances where it is reasonable to expect that the information will be held in confidence.

Confidential information will be found in a variety of formats including paper records (tender responses, some financial data, some research data, payslips, audits, employee records, member details, appraisals, occupational health records etc.) and information stored on portable encrypted devices (laptops, palmtops, mobile phones, USB memory sticks, digital images, photographs etc.). It can also include communications such as video conferencing/telephone/mobiles, general conversation and any third party confidential information.

During your work the best default position to adopt is one where you consider all information as sensitive and potentially confidential so the same standard is applied to all the information you come into contact with.

4.1 Person Identifiable Information

Information should always be considered confidential if it can be related in any way to a specific individual. The terms 'person-identifiable information' and 'personal data' are commonly used to mean any data item or combination of items by which a person's identity may be established. This can mean anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual. Essentially, if someone can be singled out in the data set then caution is needed as it is likely to be personal data. The main person-identifiable data items are:

- Forename;
- Surname;
- Date of Birth;
- Sex / Gender;
- Address;
- Postcode;
- NHS Number, hospital Number or other patient numbers; and
- Staff payroll number.
- IP address
- Locations held in cookies

Special categories of personal data as defined in the GDPR and DPA (2018) are:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination or pregnancy).

4.2 Other Confidential Information

Other information classes classified as confidential can be harder to define. The Freedom of Information Act applies exemptions to information that does not have to be disclosed by public

bodies so this can serve as a useful guide to information that should be regarded as confidential. The classes of information most likely to interest to us would be:

- Information likely to endanger an individual's health or safety;
- Information covered by legal professional privilege;
- Trade secrets; and
- Information whose disclosure would be likely to prejudice commercial interests.

The term "trade secret" is not defined in the Act although it is one that is not difficult to understand. Perhaps the most important thing to grasp is that the term can have a fairly wide meaning. Many people often think of a trade secret to be secret formulae or recipes but many of the cases considered by the courts have concerned an employer's ability to prevent the use of information about his business being used by an ex-employee. It can also cover some classes of information contained in Intellectual Property (IP) Rights such as where Pharmaceutical companies apply IP rights to their products.

A commercial interest relates to a person's ability to successfully participate in a commercial activity. In the context of the HRA for example we may hold sensitive information for regulatory purposes e.g. commercial information in Research Applications.

5 Corporate Level Procedures

5.1 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 the Caldicott Guardian and DPO.

- Any instances where personal or confidential information has been disclosed inappropriately must be reported using the HRA's Information Governance Breach form.

The HRA 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 Information Governance Staff Handbook, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data in line with the Information Commissioner Office (ICO's) Anonymisation: managing data protection Code of Practice.

Access to rooms and offices where laptops 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. Printouts must not be left lying around but be filed and locked away when not in use.

The HRA 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.

5.2 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

- When the information is required by law or under a court order. Some statutes, such as the Freedom of Information Act and requests from the Police, will require us to disclose information. In this situation staff must escalate to the data@hra.nhs.uk inbox. The Information Governance & Complaints Team will then consult the DPO 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 escalate to the data@hra.nhs.uk inbox. The IG & Complaints Team will then consult the Caldicott Guardian and DPO if necessary before advising.

- For any proposed routine disclosures of personal/confidential information, please complete the Data Protection Impact Assessment (DPIA) screening template to determine whether a full DPIA should be undertaken.

If staff have any concerns about disclosing information they must raise in the first place with the IG & Complaints Team by e-mailing the data@hra.nhs.uk inbox. The Team will then consult the Caldicott Guardian and the DPO 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 IG and Complaints Team.

Staff must ensure that appropriate standards and safeguards are in place to protect against inappropriate disclosures of confidential personal data.

5.3 Transferring personal data or other confidential information by email.

The HRA EOL email service is a secure service, this means it is authorised for sending sensitive information, such as personal or confidential data.

The most secure and only route to send emails is using HRA EOL email address as information is automatically encrypted. Email addresses that are considered secure for sending sensitive information (meet the same high accreditation and security standards as hra.nhs.uk) are:

- nhs.net
- secure.nhs.uk
- Gov.uk
- cjsm.net
- pnn.police.uk
- mod.uk
- parliament.uk

If you need to send an email to a third-party not on any of the above secure email address you must follow the steps below to encrypt the email:

- Double check the recipient details are always correct (this is a high-risk breach error)
- Add the word [Secure] into the subject line of the message using square brackets
- All attachments are automatically encrypted however if you are sending confidential information you should also password protect the attachment and send a separate email with the password once the correct recipient has confirmed receipt.

5.4 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 HRA information with them which could be confidential in nature e.g. on a laptop or paper documents.

Taking home/removing paper documents that contain person-identifiable or confidential information from HRA 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 HRA locations staff must ensure that their working practice complies with HRAs policies and procedures.

Using electronic removable media is not permitted at the HRA.

Staff must minimise the amount of person-identifiable information that is taken away from the HRA.

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

If staff are working whilst travelling e.g. on a train, care should be taken with regard to what other travellers may oversee or hear and personal identifiable or confidential information should not be visible or discussed. Privacy screens can be used to reduce the likelihood of screens being viewed by another individual.

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.

5.5 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, printouts, 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.

5.6 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 the HRA.

If staff have concerns about this issue they should discuss it with their Line Manager, IG & Complaints Team or DPO.

5.7 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 Quality Assurance Team in collaboration with site owners.

6. Distribution and Implementation

6.1 Distribution Plan

This document will be made available to all staff via the HRA Atlas. A notice will be issued in HRA news notifying of updates to the document.

6.2 Training Plan

All staff are required to complete the ESR Information Governance and Data Security training annually. In addition, information asset owners are required to complete IAO training provided by NHS Digital.

7.Management of Documents and Records

The documents will be managed in line with the HRA's Record Retention Schedule.

8.Supporting documents

- Data Protection Impact Assessment Procedure and Template
- Freedom of Information Policy & Procedure
- Data Subjects Rights Requests Procedure
- HRA Security EAT Framework
- HRA Acceptable use of ICT user obligations
- HRA IG Staff Handbook
- HRA Information Security Policy
- HRA Information Security Breach procedure and form

9.Dissemination and publication of the document

A copy of this document is held in the HRA Atlas. All members of staff are expected to read and understand the information security policy as part of their HRA induction and when revised versions are released. This should be confirmed as part of the annual appraisal process.

Screening Questions - HRA Equality Analysis and Privacy Impact Assessment

Equality and privacy screening questions

Equality and Privacy Assessments
For every HRA policy (defined by the Equality and Human Rights Commission as a function, strategy, procedure, practice, project or decision), please ensure the following assessments have been completed:

Assessment	Screening question	Answer	Action required
Equality	Has an Initial Equality Impact Assessment been carried out?	Yes	If no, please do so now. Do not publish the policy until the EIA is ready to be published alongside it.
Privacy	With due regard to the Data Protection Act, does this policy involve the use of Personal Information?	no	If yes, please complete an Initial Privacy Impact Assessment. If no, no further action is needed.

Document Control

Version Number & Status	Date of Change	Reason for Change
2.0	27/11/20	IGSG suggested changes to scope
2.1	20/01/2021	Updated for accessibility
3.1	09/05/22	Change to HRA Atlas
3.2	24/01/2023	Regular review

Reviewers

Name (name of reviewer and/or management group reviewing)	**Version Reviewed**
IGSG	2.0
IGSG	3.2

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 The Health Research Authority
- 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 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

The Health Research Authority 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 the Health Research Authority, who may be held personally accountable for any breaches of information security for which they may be held responsible. The Health Research Authority 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.