Royal Free London NHS
NHS Foundation Trust

Patient and Staff Confidentiality Policy

Version:	5.0
Ratified by:	[redacted] Chief Information Officer
Date ratified:	05.06.2019
Name of originator/author:	• Data Protection Officer & Head of IG (Deputy CIO) • IG manager
Name of responsible individual:	• Senior Information Risk Owner • Caldicott Guardian • Information Governance Manager • Data Protection Officer & Head of IG (Deputy CIO)
Date issued:	02.07.2018
Review date:	02.07.2019
Target audience:	Trust employees, voluntary staff, students, staff on honorary contracts, contractors and all other staff with access to staff and patient personal confidential data.
Intranet:	http://freenet/trustpolicies.asp
Related policies:	Information Governance Overarching Policy Information Security Policy Information Risk Policy Mobile Devices and Remote Access Policy
Date equality impact assessment completed.	Yes

Version Control Sheet

Version	Date	Author	Status	Comment
0.1	12-05-2014	[redacted]	Draft	Harmonised RFL /BCF policy.
0.2	23-05-2014	[redacted]	Draft	Revision of responsibilities.
1.0	09-06-2014	[redacted]	Previous version	Minor revisions and rectifying typos, following review by IGG.
2.0	13-01-2015	[redacted]	Previous version	Updated staff responsibilities section following review by IGG
3.0	23-06-2015	• [redacted], SIRO • [redacted], IG officer	Previous version	New guidance for the safe transfer of paper health records/PCD between sites and home. Agreed IGG June 2015.
3.1	10-12-2015	• [redacted], SIRO • [redacted], Information Governance Manager • [redacted], Head of Information Governance and Coding (Data Protection officer)	Previous version	General updates including contacts page. Added guidance on: Voicemail messages Confidential waste NHSmail [secure] service
3.2	10-05-2016	Authors same as v3.1	Previous version	Added guidance: Bulk emailing Protecting PCD during department moves Mobile ‘apps’ Information sharing opt-out
3.3	04-08-2016	Same as v3.1	Previous version	Policy reviewed by IG group and agreed. Added guidance on video conferencing applications.
4.0	22-05-2017	• Senior Information Risk Owner • Caldicott Guardian • [redacted], Information Governance Manager • [redacted], Head of Information Governance and Coding (Data Protection officer)	Previous version	Updated to include further guidance regarding staff PCD, social media and other general updates. Policy name updated to ‘Patent & staff confidentiality policy’.
5.0	23-05-2018	• Data Protection Officer & Head of IG (Deputy CIO) • IG manager	Live	Updated to include General Data Protection Regulation

Contents

The trust is committed to the delivery of world-class care and expertise to both staff and patients, and our values of being positively welcoming, actively respectful, visibly reassuring and clearly communicating are fundamental to the delivery of this. This policy has been developed with our values in mind, and is intended to be implemented within the spirit of these values.

1. Introduction

Everyone working for the National Health Service (NHS), including staff, volunteers, contractors and temporary (bank) staff, are under a legal duty to keep patient and staff information, held in whatever form, confidential and secure. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence, the Data Protection Act (DPA) and General Data Protection Regulation (GDPR). It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information. The above staff groups are also required to comply with the requirements of the NHS Code of Practice: Confidentiality (Code of Confidentiality).and HSCIC Code of practice on confidential information.

This policy applies to all patient and staff information, including those who are deceased, however held or stored (paper, electronically, photographically) and for whatever purpose it is used (delivering care, research, teaching, management and planning).

As with patient information, it is the responsibility of every member of staff to ensure that **staff information** is kept safe and secure at all times and that confidentiality is safeguarded. This applies particularly to the Workforce department, and departmental managers who maintain personal files on members of staff.

All staff should ensure that they are aware of the procedures to be followed for confidentiality issues that may arise in their area of responsibility.

2. Policy statement

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within the Trust and have access to personal data. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. This policy provides the framework within which the trust will ensure compliance with relevant legislation.

3. Definitions of terms used

Accountability means there is an expectation that privacy is afforded by design and by default. All new systems should be designed in accordance with privacy by design and privacy by default (refer DPIA appendix). The Trust must keep a record of processing eg. through data flow mapping exercises.

Anonymised Information - information from which individuals cannot reasonably be identified. Names, addresses, full postcodes or identification numbers, alone or together or in conjunction with any other information held by or available to the recipient, can be used to identify patients so these items should never be included in anonymised data

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person,

which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (eg. fingerprint) data.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
The data subject has the right to withdraw consent at any time. It must be as easy to withdraw as to give consent.

Consent to receive care – Explicit or Expressed. This means articulated patient agreement. The terms are interchangeable and relate to a clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.

Consent to receive care – Informed. The patient must be given full information about what the treatment involves, including the benefits and risks, whether there are reasonable alternative treatments, and what will happen if treatment does not go ahead. Healthcare professionals should not withhold information just because it may upset or unnerve the patient.

Consent to receive care – Implied. Patient agreement that has been signaled by behavior of an informed patient.

Consent to receive care – Voluntary. The decision to consent or not consent to treatment must be made alone, and must not be due to pressure by medical staff, friends or family.

Cross-border processing means either:
(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Data Controller, Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

Data Processor, Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Protection Legislation means: (i) the GDPR and any applicable national implementing Laws as amended from time to time (ii) the DPA to the extent that it relates to processing of personal data and privacy; (iiii) all applicable Law about the processing of personal data and privacy.

Disclosure - the divulging or provision of access to data. This may only take place where there is a legal basis to make such disclosure

DPA means the Data Protection Act, 2018

DPIA – Data protection impact assessment – this is required where processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing.

Encryption - the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing a password or key.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

GDPR: the General Data Protection Regulation (Regulation (EU) 2016/679).

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Information Sharing Agreements - documented rules and procedures for the disclosure and use of patient and staff information that specifically relate to security, confidentiality and the destruction of data, between two or more organisations or agencies.

Lawfulness of processing means processing shall be lawful only if and to the extent it conforms to Article 6 of the GDPR. See Appendix

LED: means Law Enforcement Directive (Directive (EU) 2016/680)

Main establishment means:
(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.

Personal Confidential Data (PCD) - describes personal information about identified or identifiable individuals, which should be kept private or secret. ‘Personal' includes the Data Protection Act (DPA) definition of personal data, but includes data relating to the deceased as well as living people, and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include

'sensitive' as defined in the DPA. Examples of identifiable data are: names, address, postcode, date of birth and NHS Number and **includes patient and staff information**.

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Picture Archiving and Communication System (PACS) - consists of all digital, computer-generated x-ray images as opposed to the analog film. Additionally, PACS acts as a digital filing system to store patients' images in an organised way, which enables records to be retrieved and shared with ease.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Public interest - exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest.

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Safe Haven - an agreed set of arrangements that are in place in an organisation to ensure confidential personal information (e.g. patients and staff information) can be communicated safely and securely.

Sensitive Personal Information - The GDPR refers to sensitive personal data as “special categories of personal data”.
The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

4. Equality statement

The Royal Free London NHS Foundation Trust is committed to creating a positive culture of respect for all individuals, including job applicants, employees, patients, their families and carers as well as community partners. The intention is, as required by the Equality Act 2010, to identify, remove or minimise discriminatory practice in the nine named protected characteristics of age, disability (including HIV status), gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation. It is also intended to use the Human Rights Act 1998 to treat fairly and value equality of opportunity regardless of socio-economic status, domestic circumstances, employment status, political affiliation or trade union membership, and to promote positive practice and value the diversity of all individuals and communities.

This document forms part of the trusts commitment, you are responsible for ensuring that the trust's policies, procedures and obligation in respect of promoting equality and diversity are adhered to in relation to both staff and service delivery.

The equality analysis for this policy is attached at Appendix J.

5. Responsibilities

5.1 Information governance management

Organisational and managerial structures that support appropriate consideration of information governance issues are essential to a properly managed information governance assurance programme that sustains continual improvement. The trust has established clear lines of accountability throughout the organisation for information governance management that lead directly to the board.

The trust's senior information risk owner (SIRO) chairs the information governance group and will be responsible for reporting progress quarterly to the patient safety committee, which is an assurance committee of the board.

The trust has a Data Protection Officer (DPO) whose job is to assist in monitoring internal compliance, informing and advising on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acting as a contact point for data subjects and the Information Commissioners Office.

5.2 Staff

Staff must ensure that all information relating to identifiable individuals (PCD), including patient and staff data, is kept secure at all times. All staff must adhere to the following trust rules:

Information security

- You must ensure that portable devices that you use for storing and transferring personal confidential data are encrypted, this includes laptops, USB memory sticks, CDs, tablets/iPads, smartphones, external hard drives etc.
- Personal confidential data must not be saved to the 'C' drive of a workstation PC; the 'C' drive is unsecure and unencrypted. Instead staff should save personal confidential data to their secure network server drives.
- Never share passwords to systems with anyone, and always log out of computers when not in use.
- Think about who has access to the data that you hold - how easy would it be for an

unauthorised person to access it?

- Be prepared to challenge people entering your work area if you do not recognise them or if they do not have ID displayed.
- When carrying confidential data (such as patient handover details), ensure it is secure so that no data can be seen or dropped.
- Never leave any trust information unattended in a car; this includes computer devices holding data and paper records
- If you have to email personal confidential data use your NHS.net email account. But remember that only NHS.net to another NHS.net account is encrypted and secure.
- Ensure fax numbers are correct and up to date. If the recipient data is extremely sensitive send a test fax first to ensure you are using the correct number. Before sending the document, ask the recipient to confirm safe receipt. FAX transmissions are to be actively discouraged, in favour of secure email.
- When sending personal data in the post (e.g. to patients), ensure it is sent in a strong envelope and securely sealed. If sending large quantities of highly sensitive information, ensure the data is double wrapped and send by recorded delivery or if appropriate by courier.
- Never disclose personal confidential data over the telephone unless you are certain that you are speaking to the intended person.
- When personal confidential data is no longer required, ensure it is securely destroyed (e.g. paper into one of the confidential waste bins, and hand all redundant electronic hardware to the IT department for redeployment or destruction).

Access controls

- Staff must never share access controls such as smartcards*, barcodes, swipe cards, ID badges, proximity cards, door codes and access codes.

Discussing confidential information

- Never discuss confidential, sensitive or personal confidential data in public areas, lifts, the tube, buses or a restaurant, or other public places
- Be aware of who could overhear your conversation. If you work at a reception desk ask the patient to state their own details to ensure you do not accidentally read out details of another patient.
- Never discuss patient data with friends and family outside work.

Social media (e.g. Facebook, WhatsApp & Twitter)

Social media are web-based applications that allow people to create and exchange content including text, images, videos and sound recordings. Examples of such applications include (but are not limited to) Facebook, WhatsApp, Twitter, LinkedIn, YouTube, Google+, Instagram, Snapchat, Vine, Viber and LINE. Staff must not use social media to share or store trust PCD including patient and staff data, this also includes web-based social media applications that claim to provide encryption.

A limited number of other clinical web-based applications have been approved by the trust for the purposes of viewing and exchanging PCD, a list of these are available from information governance.

Staff must ensure that they observe the following rules regarding the use of social media.

- Staff must not release any PCD on social media which they have obtained as part of their job role.
- Staff must not discuss any aspect of patient care on social media, even if they

believe they are conversing with the actual patient.

- Images must not be taken by staff on personal devices (such as smart phones/cameras) except with the explicit (written) consent of the individual(s) in the image. Under no circumstances may these images be posted or exchanged on social media.
- Staff are permitted to use social media to discuss non PCD related trust matters such as rota and shift swaps.

See also:
Doctors' use of social media (GMC)
Guidance on using social media responsibly (NMC)

Photographic images

- Staff must ensure that images of patients stored on a trust memory card or camera are immediately transferred to a secure network drive and then deleted from the devices. All trust cameras and unencrypted storage media/cards must be held in a secure location at all times. For further guidance please see the trust's Photography and Video Recording of Patients Policy and Procedure

- All photographic images taken are subject to Trust policy and DPA / GDPR on Consent.

Cloud data storage services

- Staff must not upload or store personal confidential data/ business confidential data to cloud services such as Apple iCloud, Google Drive, Microsoft OneDrive etc. The trust cannot guarantee the security of these cloud services or the country in which the data is stored.

The above list of rules is not exhaustive, there are many different everyday scenarios where PCD is handled, stored, accessed, disclosed, transferred and all staff must ensure that PCD is handled appropriately and securely at all times.

Failure to apply controls in handling personal data and/or failure to follow the guidelines and legislation as outlined in this policy could result in a member of staff facing disciplinary action. A copy of these procedures are available on freenet and from the Workforce Department.

*For A+E staff only it is understood that some minimal level of sharing may be necessary until faster processes are developed.

Information governance training

- All staff must undertake mandatory annual information governance training (eLearning)

6. What is personal confidential data (PCD)?

A duty of confidence arises when a patient shares information with trust staff in circumstances where it is reasonable to expect that the information will be held in confidence. It

- is a legal obligation under data protection legislation
- is a requirement established within professional codes of conduct
- must be included within NHS employment contracts as a specific requirement linked to disciplinary procedure

It is essential, if legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service.

A duty of confidence also arises when a trust staff member shares their personal information with the trust, for instance during an interview process or information provided to the trust in the course of employment which is then held by the Workforce department.

7. Consent for disclosure and use of personal confidential data

Consent must be obtained from the patient or staff member, prior to personal data being recorded by the Trust, where non-direct care activities and data processing are involved.

Information provided should not be used or disclosed in a form that might identify a patient or member of staff, for any purpose, without his or her consent for such purpose(s). Refer to Appendices B and C, covering data processing and lawfulness.

Information that specifically identifies an individual patient includes:

- name
- address
- photographs or videos

Staff should avoid quoting other details that may, especially in combination, enable an individual to be identified, such as:

- full postcode
- date of birth
- telephone number
- email address
- uncommon diagnosis or treatment

7.1 Patient consent and disclosure

Information that can identify individual patients must not be used, shared or disclosed for purposes other than direct care without the individual's explicit consent, or other lawful basis.

7.1.1 Explicit consent for research purposes

Researchers must seek explicit patient consent for patient participation and information processing for research and development projects that will involve them personally. The original signed consent form must be kept on file, and may be audited.

Where patients have been informed of the following:

- the use and disclosure of their information associated with their healthcare
- the choices that they have and the implications of choosing to limit how information may be used or shared

then explicit consent is not usually required for information disclosures needed to provide that healthcare.

7.2 Disclosure without consent

Disclosing patient information without the patient's consent can be justified in particular circumstances, for example:

- if there is an overriding patient or public interest
- where required by a court order or statute
- there is a registered exemption under section 251 of the NHS Act 2006
- covered by "lawful processing" for patient care

7.2.1 Patient / public interest

Occasionally, in the best interests of the patient, other individuals or the general public, staff may, having conferred with others including at least a senior clinician, disclose information against the wishes of the patient/family. Any objections to such disclosures should be recorded in the case note.

In general, it would be in the public interest to disclose personal information in order to prevent serious crime and to support its detection, investigation and punishment. Serious crime is usually regarded as crime that puts someone at risk of death or serious harm, that could cause serious harm to national security or public order, or crime involving substantial financial gain or loss. Staff disclosing information to the police should provide the minimum necessary, and keep a record of the disclosure. The patient concerned should be informed of the disclosure, but not if that would defeat the purpose of the investigation or allow a potential criminal to escape or put staff or others at risk. Where staff are uncertain they should seek advice from a senior manager, and from the trust's legal officer if necessary.

Patients generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right.

7.3 Patient awareness of the use of their personal information

Patients must be made aware that the information they give may be recorded, shared in order to provide them with care and may be used to support clinical audit and other work to monitor the quality of care provided.

Patients will be made aware of the use of their information during interactions with staff and also via the trust's patient information leaflet and/or privacy statement. These documents explain to patients typically how their information is recorded, shared and how patients may express concerns. The leaflet and privacy statement are available on the trust website and should be printed and given to patients whenever appropriate. Additionally, statements in patient handbooks and by health care professionals providing care and treatment will remind patients of the use of their personal information to support their immediate care and the delivery and planning of care for others, including teaching and research and development.

Click on the link below to view the: Trust privacy statement

8. Storage of personal confidential data

8.1 Electronic storage of records

PCD must only be stored on the trust's secure network and on trust approved encrypted devices / media. The encryption standard must meet the DoH technical standard which at the time of writing is AES-256.

Databases holding personal confidential data must be registered with the IM&T directorate, which maintains a register of such databases, including the names of those responsible for the security of each of them.

All redundant electronic media, which may or may not hold PCD, must be handed to IT for secure certified destruction. No IT equipment must leave the trust premises without being checked by IT for PCD. Examples include floppy disks, desktop computers, laptop computers, desktop printers, compact discs (CDs), Digital Versatile Disc (DVDs) photocopier printers, external hard drives, PC hard drives, USB memory sticks, dictaphones, audio tapes, mobile / smart phones, tablets or any IT equipment capable of storing data. Please contact the IT Service Desk on 020 3758 2020 for further information.

All department medical devices must be checked by the trust's medical electronics department for PCD assessment prior to return to the manufacturer/leasing company/or leaving the trust. Medical devices often store PCD which must be assessed and if required extracted by the department/service for data retention. The PCD can then be removed by the medical electronics department before leaving trust premises. Please contact the Medical Electronics Department on x33197 for further information.

Files and disks containing PCD should be stored securely, access restricted and preferably not held by patient name.

The loss or theft of any IT equipment or media must be reported immediately using the online Datix incident reporting system, the trust's data protection officer and security team must also be notified.

Staff members with smartcards should act in accordance with the NHS Care Record Service smartcard terms and conditions (Registration Authority).

See also: Registration Authority Policy and Procedure

8.2 Manual storage of records

Manual records, including patient or staff information, must be held in secure storage with clear labelling.

Patients' paper case notes must be kept securely, including when in wards and clinics, and in transit within or between sites. Case notes and other personal confidential data should not be left unattended during the working day or overnight.

Medical records can be stored outside patients' rooms in unlocked wall mounted patient folder holders however ward staff must observe the following rules:

- access to the ward is controlled e.g. locked, swipe access, intercom, CCTV etc
- ward staff wear trust identification badges at all times
- visitors/members of the public entering the ward are politely challenged.

Staff should only take patient or staff records home in exceptional circumstances, service operational managers/information asset owners should be made aware of this practice. **See sections 11.8 and 11.9 for further guidance on this.**

8.3 Accessing and storing data on cloud services

Staff must not upload or store personal confidential data and business confidential data to cloud services such as Apple iCloud, Google Drive, Microsoft OneDrive etc unless explicitly approved by the trust's Data Protection Officer.

The trust cannot guarantee the security of these cloud services or the country in which the data is stored.

Currently the trust provides limited user access to Dropbox for the storage of documents that do not contain PCD or are not commercially sensitive. The user will need to request access via their manager – this will then need to be authorised by the trust's data protection officer. The confirmation email will contain a 'Code of Conduct', which the user will need to accept before access is granted.

8.4 Mobile device applications or 'apps'

A limited number of clinical web-based applications have been approved by the trust for the purposes of viewing and exchanging PCD, a list of these are available from information governance.

If a member of staff believes that there are clinical apps or other technologies that could benefit their patients, this should be discussed with the information governance team. An app must not be used to store PCD unless it has been approved by the information governance team and or the information governance group.

Staff must not use social media to share or store trust PCD including patient and staff data. See section 5.2 for further guidance.

9. Sharing personal confidential data

Safe and effective care is dependent upon relevant confidential information being shared amongst all those involved with caring for an individual. All staff with regard to sharing information should abide by the following national rules:

- Members of a care team should share confidential information securely when it is needed for the safe and effective care of an individual.
- Information that is shared for the benefit of the community should be anonymised.
- An individual's right to object to the sharing of confidential information about them must be respected.

Special rules about sharing patient information apply in matters where child protection issues may be involved. Staff must obtain advice on this from professional colleagues working in child protection (safeguarding children and adults team).

9.1 Sharing information with organisations (information sharing agreements)

Under the NHS 'Care Records Guarantee' trust staff may pass on appropriate patient information only to people or organisations that have a genuine need to see or use that

information (on a 'need to know' basis). The Caldicott principle 7 supports this. Examples of such need include clinical care, clinical audit, protecting health, managing the service, investigating concerns, teaching and research and some other essential functions. Staff must take measures to ensure that the individuals or organisations are entitled to receive the information, and they are responsible for sending the information in a way that safeguards confidentiality

The trust has developed information sharing agreements that set out the standards and procedures that should apply when disclosing confidential patient information with other organisations and agencies.

Information sharing agreements can be a useful way of outlining the standards that each party to an agreement will adopt. However, they do not in themselves provide a lawful basis for sharing confidential information. That can only result from effectively informing the person whose information it is about the possibility of sharing and the choices they have to limit sharing. If the individual says no to sharing, then confidential information may only be shared in exceptional circumstances.

For clarity, an information sharing agreement is not required where the sharing is for an ad-hoc request for information.

Information sharing agreements should be prepared by information asset owners responsible for clinical services with working links with external organisations (such as other NHS bodies, local authorities and other statutory organisations and charities). Either the trust's standard template information sharing protocol on freenet, or a nationally approved template, must be used. The Caldicott guardian and data protection officer, who must sign each such agreement to authorise the data flow, will from time to time review flows of information to external organisations that are directly involved with patients.

Data sharing portal (database of information sharing agreements)

The trust's data sharing portal (DSP) is an online database of approved information sharing agreements between the trust and third parties. The portal allows staff to access copies of the agreements that have been shared and approved by information governance and the Caldicott Guardian.

Each ISA has a 'subscriber', this is the staff member from the speciality/department who originally entered into the agreement. It is the responsibility of the subscribers to ensure that the ISA's are kept up to date and are renewed in advance of their expiry date.

To access the data sharing portal and further information see freenet guidance

9.2 What can be shared?

The minimum amount of information necessary to provide safe care or satisfy other purposes can be shared. This must be clearly balanced against the need to provide safe care where missing information could potentially compromise the quality of care provided. It is important to consider how much information is needed before disclosure. Information asset owners can use a range of measures to make it more difficult for unauthorised persons to identify patients from records or other system reports or data transfers. The measures outlined below offer a range of levels of protection:

- full anonymisation of information

- pseudonymisation – anonymised data that includes a reference that can be used to derive personal information from another data source, for example NHS number
- hospital number with or without date of birth

Anonymised information is not confidential and may be used with relatively few constraints.

When anonymised or pseudonymised information is shared, care should be taken to ensure that the method used is effective and individuals cannot be identified from the limited data set e.g. age and postcode together could be sufficient enough to reveal an individual's identity. The use of initials to try to disguise a name is ineffective and does not provide any level of identity protection.

For further guidance on anonymisation and pseudonymisation please contact the trust's Data Protection Officer x35137.

9.3 Objections to data sharing

Patients have the right to object to their information being used and shared, unless there is a legal basis that overrides an individual's objection such as for example the public interest. Such patient requests must be sent to the trust's data protection officer for investigation.

9.4 Patient privacy notice

A privacy notice providing information to patients about how the Royal Free London NHS Foundation Trust handles their personal data is available on the trust's website here . This will be reviewed on a regular basis by the information governance group.

10. Right to access personal confidential data

10.1 Staff members accessing records

Staff members are not permitted to gain access or attempt to gain access to information they do not need to see to carry out their work. This includes viewing the personal data (or sensitive personal data) of family members, colleagues, celebrities, friends or neighbours.

Accessing a patient or staff record (which may include records relating to their colleagues) without authorisation is a breach of trust policy (based on DoH guidance), a breach of patient confidentiality and a criminal offence if data is 'knowingly or recklessly' obtained or disclosed for non-work related purposes or personal gain.

A prosecution is likely if the following can be proven:

- A patient's records are compromised and the patients were not at any time under the medical care of the individuals accused of accessing the records inappropriately.
- The accused has no work-related reason to access records.
- The individual accesses the information for personal gain without consent from the trust.

The offence is punishable by way of a financial penalty of up to £5,000 in a Magistrates Court or an unlimited fine in a Crown Court.

Such breaches of patient confidentiality will where appropriate be dealt with under the trust's disciplinary procedures. In the case of clinical staff the trust may at its discretion refer the matter to a professional body (e.g. GMC or NMC) for further investigation where the member of staff can face further sanctions, which may include being struck off. If the incident is deemed sufficiently serious the trust may also refer the matter to the Police.

If a member of staff suspects possible breaches of confidentiality or abuse of patient data, then they must immediately raise these concerns with their line manager or other appropriate colleagues, e.g. the information governance manager/Caldicott guardian/senior information risk officer and complete a Datix incident form immediately which can be accessed via a trust PC. **The Trust has an obligation to report data breaches to the ICO within 72 hours. All data breaches must be reported by staff within 24 hours of any breach coming to light.**

The relevant incident manager will manage the investigation of the incident, including ensuring that the incident is brought to the attention of the relevant senior divisional or directorate managers, the data protection officer, and for serious incidents, the Caldicott guardian and the senior information risk owner (details in appendix D). The incident will be recorded on the STEIS system. See also Information Risk Management Policy and Incident reporting and learning (including serious incidents and never events) policy

The information governance group reviews all breaches of patient confidentiality, and the more serious categories are published in the trust's annual report and IG toolkit.

If staff wish to access their own personal medical or staff records which are held by the trust they must do so by submitting a subject access request to the appropriate department. If a staff member wishes to access their own records directly via trust records systems (ie. not via subject access procedure) they must first seek approval from the Data Protection Officer.

Staff who access their own personal medical or staff records without authorisation on a persistent basis will where appropriate be subject to the trust's disciplinary procedures.

10.2 Subject access request – patient records

When dealing with patients and their families the focus should be on sharing information as a natural part of the care process rather than patients having to resort to formal processes to gain access to information held about them.

The trust will, where appropriate, provide patients with ready access to information that it holds about them, whether held in manual or electronic format, in line with the provisions of the GDPR, the Data Protection Act 2018, Access to Health Records Act 1990, and the Health and Social Care Act 2001.

The medical records department manages patient subject access requests. The GDPR requires that all access requests must be responded to by the Trust within one month of receipt of the request. Unless special circumstances prevail, the request is serviced by the Trust free of charge to the patient.

10.3 Subject access request – staff records

All staff have the right to access records about them held by the trust. These rights are embodied within the DPA andGDPR, Access to Medical Reports Act 1988 and the

Human Rights Act 1998. Staff do not have to give reasons for seeking access to their own personal records.

Staff wishing to access records held about them should contact the Workforce department (employee relations) [redacted] who manage staff subject access requests.

All staff have the right to obtain from the Trust (the controller) confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and information on where, how and by whom the data is being processed.

In addition to access requests, legislation also requires the Trust to observe:

Right to rectification

Staff have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

Right to erasure ('right to be forgotten')

Staff have the right to obtain from the Trust the erasure of personal data concerning him or her without undue delay and the Trust has the obligation to erase personal data without undue delay for a range of reasons, including where holding or processing these data are no longer valid, or do not comply with law. Where data has been shared with other controllers, the Trust is required to take reasonable steps to inform controllers which are processing the personal data that the data subject has requested the erasure.

The right to erasure may be denied by the Trust for reasons of public interest in the area of public health and in meeting its legal obligations.

10.4 Deceased patients

The law on releasing information about deceased patients is in the Access to Health Records Act 1990. Under this legislation the patient's personal representative or executor or administrator, or anyone having a claim resulting from the death (this could be a relative or another person), has the right to apply for access to the health records. If the deceased person had indicated that they did not wish information to be disclosed, or the record contains information that the deceased person stated should remain confidential, then it must remain so. The trust can deny or restrict access if it is felt that disclosure would cause serious harm to the physical or mental health of any other person, or would identify a third person.

10.5 MPs

Special arrangements apply to requests for information about patients from their elected representatives, such as Members of Parliament (MPs). If in doubt about how to proceed, contact the director of corporate affairs and communications or the data protection officer.

10.6 Media enquires

All media enquiries about individual patients should be referred without comment to the communications team. Further advice is available on freenet.

11. Sending, receiving and transporting confidential information

11.1 Couriers

On the rare occasions when PCD needs to be physically sent in paper or electronic format to an address outside the trust, it is important an approved courier is used to deliver the device or paper. All media containing PCD must be encrypted before physically leaving the trust and the password communicated separately. Paper PCD must be placed in a secure and sealed envelope. The PCD must be signed for on collection and delivery to keep an audit trail. The hospital reception desks hold a list of approved couriers.

11.2 Telephone

All possible steps must be taken to ensure that PCD is not divulged over the telephone to anyone without authority. Staff should check that any callers, by telephone or in person, are who they say they are and that they have a legitimate right to have access to that information. Confirmation of the person can be obtained by asking certain personal details, such as:

- date of birth
- address and post code
- appointment dates
- hospital or NHS number

11.3 Voicemail/answer machine telephone messages for patients

Staff must ensure that if they are leaving a telephone message for a patient on an answering machine/voicemail that they only disclose the name of the hospital, their name and a number for the patient to call back on. No clinical information such as the department/speciality should be disclosed.

11.4 Email

Emails sent from an NHSmail address to another NHSmail address are secure and may if necessary contain the minimum PCD. This includes emails sent between trust staff.

Information sent via a non NHSmail address which is transmitted on the internet is not secure and should therefore be regarded as no longer confidential. This includes information sent to and from UCL email accounts eg. @ucl.ac.uk. Therefore, if trust staff need to use internet email to communicate about patients, then the data must either be anonymised or encrypted; password protection of attachments is insufficient (or use the NHSmail [secure] service see section 11.5 below). Date of birth may be sent with anonymised data as confirmation of identity in order to reduce the risk of misidentification of a particular patient. Staff must not send frank identifiers (name, address, postcode, phone number) over the internet. Names or initials of patients should never be typed into the subject line of emails, whether external or internal.

To avoid PCD being disclosed in error staff must ensure that they have the correct email address entered for the recipients before the email is sent.

Patients are increasingly expecting that NHS staff should reply to their emails. It is recommended that replies are sent only if the patient has first confirmed that they will accept the risk that the email exchange over the internet is not secure.

Bulk emailing patients / patient email newsletters

Wherever possible patient information should be provided through the trust's website rather than sending email newsletters.

As email addresses can often identify individuals extra care must be taken by staff when emailing patients. When emailing multiple patients staff must only use the 'Bcc' field and not the'To' or 'Cc' field. The Bcc email field allows the sender to email multiple recipients without disclosing the email addresses.

If a department wishes to bulk email patients, such as a patient group newsletter, they must seek approval from information governance and their line manager before doing so. The department will be required to agree an undertaking that they will ensure that all patients email addresses are only added to the 'Bcc' field, this will then need to be double checked by at least two different staff members before sending.

11.5 Sending a secure NHSmail email to a non-secure address using the [secure] feature

NHSmail includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services such as @nhs.uk, @barnet.gov.uk, @camden.gov.uk, Gmail, Yahoo, Hotmail etc. Formatting of the message is preserved and attachments can be included.

Further instructions for staff on how to use the [secure] feature can be accessed here on freenet.

If you wish to email sensitive PCD, such as HIV data, please contact the Data Protection Officer (Head of IG and Coding) before doing so.

11.6 Fax (Facsimile transfer of information)

Fax transfer of PCD is not safe and should be avoided wherever possible. You should discourage the use of FAX in favour of secure electronic mail. Where it is necessary 'Safe Haven' procedures must be followed e.g. the number being dialled must be double checked by first contacting the recipient (unverified numbers must not be used) and receipt of the fax acknowledged. Non-receipt must be advised to the sender. Fax machines should be placed in a secure location and the room housing the machine must be locked when unattended. Refer to the trust's Safe Haven Policy for further information.

11.7 Post

When sending staff or patient PCD by post, envelopes must be securely sealed, clearly addressed to a known contact and marked 'private and confidential' and 'addressee only'. A return postcode should also be marked on the envelope. Identifiers such as the patient's date of birth, NHS number or clinic must not be visible through the letter window. Inbound mail that has not been correctly addressed and the recipient is unknown must be opened and redirected to the relevant staff member or department without delay, if in doubt staff must speak with a senior manager as soon as possible for further advice.

To minimise the risk of letters being sent to the wrong recipient or address the patient's contact details must be kept accurate and up to date at all times. This also applies to trust staff details wherever possible.

11.8 Internal mail

Correspondence and other documents containing patient or staff PCD **must** be sent in a sealed transit envelope and marked 'privateAllenvelopesandcontainingconfidential PCD should be clearly and fully addressed. If the PCD is particularly sensitive a standard sealed envelope should be used.

11.9 Digital media

All media such as compact discs and DVDs containing PCD must be encrypted and stored in a secure location at all times.

No personal confidential data should physically leave the trust in any digital media (such as a disk or memory stick) unless it is encrypted. Staff authorised to extract personal confidential data using a memory stick must use a trust approved and issued encrypted memory stick available from IT.

11.10 Transferring paper health records/PCD between sites

All staff must carefully consider the need for taking patient/client/staff records out of their base with them on a visit. This should only happen when absolutely essential and there is no other method available for accessing/recording the information required. Staff must not carry more PCD than is necessary.

It is recognised that clinical staff may find it necessary to remove patient records from their base, to assist their daily practice of seeing patients in community settings. The guidelines below should be followed to reduce the risk of the records being lost, stolen or accessed by an unauthorised person. These guidelines are also applicable to staff transporting staff records:

- When removing notes for home visits staff must ensure that they take only the notes required for those visits that are pre booked.
- Staff must consider whether the notes are actually needed in order to carry out the visit.
- PCD should not be removed for general administration purposes, e.g. writing routine reports.
- It is recommended that a record/audit trail is kept of the removal and return of health records/PCD taken from the workplace; this will assist staff in locating such documentation when required.
- Where possible, it is recommended that trust approved couriers should be used to transport health records/PCD between sites ensuring that collections and deliveries are signed for.
- Health records/PCD should be stored and carried in a secure bag/case (preferably trust green bags) marked 'Private and confidential - property of the Royal Free London NHS Foundation Trust'
- Health records/PCD should not be carried 'loosely' as this increases the risk of dropping them and losing information.
- The bag/case used to store the health records/PCD must never be left in a car when visiting, but should accompany the member of staff on each visit/into each home and never be out of sight.

Health records/PCD must not be left in unattended cars, even if they are locked in the boot.

11.11 Health records/PCD at home

This practice should only occur if the member of staff is not returning to their base after the working day or the records are required for the next working day, service operational managers/information asset owners should be made aware of this practice.

- If a member of staff is not returning to their base at the conclusion of their visits the health records/PCD must be securely stored in a bag/case and taken out of the car overnight into their home.
- Care must be taken in order that members of the family or visitors to the home cannot gain access to the health records/PCD and ensuring that they are stored in a safe location within the home e.g. away from open windows.
- Health records/PCD should not be away from the base for more than one working day i.e. if a member of staff is not returning to base at the conclusion of their working day, the records taken out on visits must be returned securely on their next normal working day.
- There may be exceptional circumstances which mean that this is not possible i.e. if a member of staff goes off sick before returning the health records/PCD. In this situation the staff member and or the staff member's line manager should arrange for the documentation to be returned as soon as is practically possible via a secure courier.

11.12 Remote access to the trust network and PCD

Please see the trust's Mobile Devices and Remote Access Policy

11.13 PCD in public areas

Staff must ensure when transporting paper documentation containing PCD such as handover sheets, that it is secure and is not visible to patients or members of the public. Extra care must be taken on public transport such as trains, tubes, buses etc. that PCD is out of view and is not unintentionally disclosed to other passengers or members of the public. Staff are advised to transport such documentation in a green trust transportation bag (see section 11.10) or an opaque secure wallet.

11.14 Protecting PCD during office / ward / department moves

It is the responsibilities of all staff involved in office moves to ensure that all PCD is transported safely and securely between locations. To ensure that no PCD (including IT equipment and medical devices) is left behind or lost in transit there must an audit trail in place for PCD so it can be tracked from one location to another.

All office / ward / department furniture must be thoroughly searched for PCD after the move and before leaving trust premises.

The trust's Decommissioning Policy and Procedure must always be followed by staff involved in office / ward / department moves. Contact the commissioning team officers for further information [redacted].

11.15 Video conferencing

The use of video conferencing applications (such as Skype, FaceTime and Google Hangouts) for consultations between staff and patients has not been approved for general trust use. At the time of updating this policy the trust were in the process of rolling out Skype for Business which has video conferencing capabilities. Requests for the installation of such applications must be made initially to the IT helpdesk, information governance will review requests on a case by case basis.

Staff must be aware that consultations that take place using video conferencing applications have the same duty of confidentiality and record keeping standards as a traditional hospital/clinic consultation.

Video conferencing is unlikely to be the right solution where the matters to be discussed may cause a patient distress or anxiety, or to discuss matters of particular sensitivity.

For more guidance please contact information governance.

11.16 Skype Instant Messaging

The trust rolled out instant messaging at the trust in 2016. Skype for Business encrypts every Instant Message and is secure for sending clinical and staff communications. It should however be treated in the same fashion as email conversations and follow the principles of the trust's Acceptable Use Policy. Like email, all conversations via Skype for Business should be work related and every message can be centrally audited. All data is stored within NHSmail UK datacentres.

Inappropriate use of Skype for Business products could result in a member of staff facing disciplinary action. A copy of these procedures are available on freenet and from the Workforce Department.

12. Disposal of personal confidential data (including paper, IT equipment and medical devices)

Information on paper relating to personal confidential data should be destroyed when no longer required using the designated confidential waste bins/consoles.

All redundant electronic media, which may or may not hold PCD, must be handed to IT for secure certified destruction. No IT equipment must leave the trust premises without being checked by IT for PCD. Examples include floppy disks, desktop computers, laptop computers, desktop printers, compact discs (CDs), photocopier printers, external hard drives, PC hard drives, USB memory sticks, dictaphones, audio tapes, mobile / smart phones, tablets or any IT equipment capable of storing data. Please contact the IT Service Desk on 020 3758 2020 for further information.

All department medical devices must be checked by the trust's medical electronics department for PCD assessment prior to return to the manufacturer/leasing company/or leaving the trust. Medical devices often store PCD which must be assessed and if required extracted by the department/service for data retention. The PCD can then be removed by the medical electronics department before leaving trust premises. Please contact the Medical Electronics Department on x33197 for further information.

Researchers must dispose of personal confidential data when it is clear that it will no longer be used for the research purpose for which it was collected.

12.1 Confidential waste overflow bags (currently Royal Free Hospital site only)

Staff must only use hessian overflow bags when the secure confidential waste consoles are full, or during an office clear-out/move. Such overflow bags, marked 'confidential waste', are only intended to be used as a temporary overflow measure and must not be a permanent method of collecting office confidential waste. If a department/office requires a permanent method of disposing of confidential waste they must place an order for a secure confidential waste console through the Facilities department. Hessian

overflow bags containing confidential waste must be kept in a secure location at all times.

13. Breaches of confidentiality

If a patient or trust staff member believes that their confidentiality has been breached they are able to pursue their grievances in the following ways:

- Refer the matter to the Trust Data Protection Officer
- Refer the matter to the Trust's complaints or PALS team
- Refer the matter to the GMC or NMC who can instigate disciplinary proceedings. This could result in healthcare professionals being struck off
- Refer the matter to the Information Commissioner's Office (ICO). The ICO is responsible for governing data protection compliance. Monetary penalties can be imposed if the GDPR is seriously contravened in a deliberate or reckless way, or of a kind likely to cause substantial distress or damages to an individual.
- Civil proceedings, which may result in paying the individual compensation
- Refer the matter to the Police which could result in criminal proceedings
- Send a formal complaint to the trust's complaints team and Data protection officer for investigation

All breaches of confidentiality must be investigated and reported on the trust's Datix system as soon as such breaches come to light, and within 24 hours.

14. Terms and conditions of employment

14.1 Employment contracts and confidentiality

All new and exisiting staff have a duty of confidentiality written into their contract and conditions of employment. Agency and contract staff are subject to the same rules.

A large proportion of staff are also bound to codes of conduct or equivalent through their professional organisations (see list at Appendix C).

Breaches of patient confidentiality will where appropriate be dealt with under the trust's disciplinary procedures. In the case of clinical staff the trust may at its discretion refer the matter to a professional body (e.g. GMC or NMC) for further investigation where the member of staff can face further sanctions, which may include being struck off. If the incident is deemed sufficiently serious the trust may also refer the matter to the Police.

14.2 Contracts with third party suppliers

Suitable confidentiality clauses are included in contracts with third parties who require access to or process PCD on behalf of the trust during the period of their contract.

All suppliers are required through the trust's NHS terms and conditions for procuring goods and services to protect the confidentiality of patient and staff information with which they come into contact.

It is a matter of law that contracts clearly state the identity of controllers and processors of data. Controllers are required to authorise processing of data under prescribed terms.

Processors are required to confirm they comply with data protection legislation and have processes in place that safeguard personal data.

Where data processing is involved by a third party, all contracts must have relevant clauses and obligations included to safeguard PCD.

Use of sub-processors must always be subject to approval from the trust.

14.3 Staff training

It is mandated that all Trust employees must complete IG training, annually. For new starters this will form part of their induction process.

14.5 Leavers

Staff leaving the trust must not take with them any PCD about patients or staff

Managers must fill out a leavers form and return this to Workforce, this will ensure that leavers no longer have network and NHSmail access. If a manager requires access to a leavers network files and NHSmail account for work purposes this can be requested through the IT helpdesk, see IT Systems Access and Usage Policy

15. Legal considerations

There are four main areas of law that constrain the use and disclosure of confidential personal health information. These are briefly described below.

1. The Common Law Duty of Confidentiality

This is not codified in an Act of Parliament but built up from case law where practice has been established by individual judgements. The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission. Whilst judgements have established that confidentiality can be breached 'in the public interest'; these have centred on a case-by-case consideration of exceptional circumstances. Confidentiality can also be overridden or set aside by legislation.

2. The Human Rights Act 1998 (HRA98)

Article 8 of the HRA98 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records.

3. The General Data Protection Regulation (GDPR)

The GDPR lays down regulations for the processing of personal data in relation to living individuals. Processing includes holding, obtaining, recording, using and disclosing of information and the GDPR applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope, e.g. it also covers staff records.

Three important aspects of the GDPR are:

- Information should only be disclosed on a strict need to know basis.
- PCD must be treated with respect, disposed of in a secure manner, and staff must not disclose information outside the line of duty.
- Legislation requires that where the Trust wishes to introduce new methods for processing personal data, then a Data Protection Impact Assessment is required to

evaluate the risk introduced by the new process. All new initiatives must include the assessment and demonstrate compliance with data protection legislation, before approval can be given and in turn the process may commence.

See Appendices section for full information on data protection legislation, including lawful processing, obtaining consent and data protection impact assessments.

Data Protection Impact Assessment

RFL has produced its own template to aid staff in undertaking DPIAs. See the DPIA template listed on Freenet

4. 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.

In addition, the following acts and guidance must also be adhered to:

The NHS Act 2006

In England and Wales, Section 251 of the NHS Act 2006 (originally Section 60 of the Health and Social Care Act 2001) provides the statutory power to ensure that NHS patient identifiable information needed to support essential NHS activity can be used without the consent of patients. The power can be used only to support medical purposes that are in the interests of patients or the wider public, where consent is not a practicable alternative and where anonymised information will not suffice.

This was developed to cover situations where informed consent could not be obtained, for example research projects of such a size as to make contacting each patient impracticable, where the public good derived from the research was agreed to outweigh the individual right to privacy.

It should be noted that although Section 251 approval can temporarily set aside the common law duty of confidentiality, compliance with the GDPR must still be maintained and data must still be fairly collected and processed – i.e. individuals have extensive rights to know who holds information about them, through which means and why. This includes identification of third parties who may be processing PCD.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Any member of staff found to have contravened this Act would be considered to have committed a disciplinary offence and be dealt with accordingly.

Health and Social Care Information Centre's Guide to Confidentiality

The guide explains the various rules about the use and sharing of confidential information. It has been designed to be easily accessible and to aid good decision-making. It also explains the responsibility organisation's have to keep confidential information secure.

16. Monitoring

Senior information asset owners will ensure compliance through yearly reporting to the senior information risk owner.

17. References

The General Data Protection Regulation EU 2016/679 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Access to Health Records Act 1990
http://www.opsi.gov.uk/acts/acts1990/ukpga_19900023_en_1

The Human Rights Act 1998
http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1

The Freedom of Information Act 2000
http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

NHS Code of Practice on Confidentiality 2003 (DoH)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

A guide to confidentiality in health and social care: Treating confidential information with respect
http://webarchive.nationalarchives.gov.uk/20160729133355/http://systems.hscic.gov.uk/infogov/confidentiality

Caldicott review: information governance in the health and care system, 2013
https://www.gov.uk/government/publications/the-information-governance-review

Records management code of practice for health and social carehttps://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

A guide to confidentiality in health and social care
http://systems.hscic.gov.uk/infogov/confidentiality

Advice about data protection from the national regulator
https://ico.org.uk/for-organisations/guide-to-data-protection/

Social media
Doctors' use of social media (GMC)
Guidance on using social media responsibly (NMC)

18. Associated documentation

- The trust's 'information governance' page on freenet for relevant policies and advice

- Other resources elsewhere on freenet via 'trust policies':
    - Media guidelines
    - Photography and Video Recording of Patients Policy and Procedure

- On the trust public website:
  - Patient privacy notice: https://www.royalfree.nhs.uk/patients-visitors/privacy-statement/

18.1 Related policies

- Mobile Devices and Remote Access Policy
- Information Governance Overarching Policy
- Information Risk Management Policy
- Safe Haven Policy
- Information Security Policy
- IT Systems Access and Usage Policy

Appendix A – Listing of key EU GDPR Articles

Article 1 "Subject-matter and objectives"

Article 2 "Material scope"

Article 3 "Territorial scope"

Article 4 "Definitions"

Article 5 "Principles relating to processing of personal data"

Article 6 "Lawfulness of processing"

Article 7 "Conditions for consent"

Article 8 "Conditions applicable to child's consent in relation to information society services"

Article 9 "Processing of special categories of personal data"

Article 10 "Processing of personal data relating to criminal convictions and offences"

Article 11 "Processing which does not require identification"

Article 12 "Transparent information, communication and modalities for the exercise of the rights of the data subject"

Article 13 "Information to be provided where personal data are collected from the data subject"

Article 14 "Information to be provided where personal data have not been obtained from the data subject"

Article 15 "Right of access by the data subject"

Article 16 "Right to rectification"

Article 17 "Right to erasure ('right to be forgotten')"

Article 18 "Right to restriction of processing"

Article 19 "Notification obligation regarding rectification or erasure of personal data or restriction of processing"

Article 20 "Right to data portability"

Article 21 "Right to object"

Article 22 "Automated individual decision-making, including profiling"

Article 23 "Restrictions"

Article 24 "Responsibility of the controller"

Article 25 "Data protection by design and by default"

Article 26 "Joint controllers"

Article 27 "Representatives of controllers or processors not established in the Union"

Article 28 "Processor"

Article 29 "Processing under the authority of the controller or processor"

Article 30 "Records of processing activities"

Article 31 "Cooperation with the supervisory authority"

Article 32 "Security of processing"

Article 33 "Notification of a personal data breach to the supervisory authority"

Article 34 "Communication of a personal data breach to the data subject"

Article 35 "Data protection impact assessment"

Article 36 "Prior consultation"

Article 37 "Designation of the data protection officer"

Article 44 "General principle for transfers"

Article 83 "General conditions for imposing administrative fines"

Article 84 "Penalties"

Article 88 "Processing in the context of employment"

Appendix B – EU GDPR principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) 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 ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Appendix C – EU GDPR requirements on lawfulness of processing, Article 6

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (This point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.)

To be noted:

The basis for the processing referred to in points (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including

measures to ensure lawful and fair processing such as those for other specific processing situations. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Also:

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Appendix D – EU GDPR requirements on processing of special categories of personal data, Article 9

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Appendix E - The Six Data Protection Principles

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; ('accuracy');

e) 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; ('storage limitation');

(f) 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 ('integrity and confidentiality').

(this is a summarised version taken from Article 5 of the GDPR)

Appendix F – The Caldicott Principles

The principles in the Caldicott Report are summarised below:

1. Justify the purpose(s) for using confidential information.

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use patient identifiable information unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary patient identifiable information

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to patient identifiable information should be on a strict need to know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to patient identifiable information should be aware of their responsibilities:

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Understand and comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

Appendix G – Professional Organisations

Below is a list of professional organisations that include a confidentiality requirement in their codes of conduct or equivalent.

- Association of Chartered Certified Accountants (Rulebook)
- Association of Operating Department Practitioners (Code of professional conduct)
- British Association of Occupational Therapists (Statement of conduct)
- British Dietetic Association (Code of Professional Conduct 2008)
- Chartered Institute of Personnel and Development (Code of professional conduct)
- Chartered Institute of Public Finance and Accountancy (Standard of professional practice on ethics)
- Chartered Society of Physiotherapy (Rules of professional conduct and core standards of physiotherapy practice)
- Dental Nurses Standards and Training Advisory Board (Code of ethics)
- General Medical Council (Confidentiality: protecting and providing information)
- Health Professions Council* (Standards of conduct, performance and ethics)
- Medical Laboratory Technicians Board (Statement of conduct)
- Nursing and Midwifery Council (The Code: standards of conduct, performance and ethics for nurses and midwives)
- Royal College of Radiographers (Code of professional conduct)
- Royal College of Speech and Language Therapists (Compliance procedure)
- Royal Pharmaceutical Society of Great Britain (Code of ethics and professional standards)

The Council regulates the following professions: arts therapists, biomedical scientists, chiropodists/podiatrists, clinical scientists, dietitian, occupational therapists, operating department practitioners, orthoptists, paramedics, physiotherapists, prosthetists/orthotists, radiographers and speech and language therapists.

Appendix H – Data Protection Impact Assessment

Article 35 of the EU GDPR, "Data protection impact assessment", states:

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

> (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
>
> (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
>
> (c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

RFL has produced its own template to aid staff in undertaking DPIAs. See the DPIA template listed on Freenet.

Appendix I – Contacts

Name	Role	Email	Contact details
[redacted]	Data Protection Officer, Head of Information Governance and Deputy CIO	[redacted]	[redacted]
[redacted]	Caldicott Guardian	[redacted]	[redacted]
[redacted]	Information Governance Manager	[redacted]	[redacted]
[redacted]	Senior Information Risk Owner	[redacted]	[redacted]

Appendix J- Equality analysis

An equality analysis is a review of a policy, practice, function, business case, project or service change, which establishes whether there is a negative effect, or impact on particular social groups. This In turn enables the organisation to demonstrate it does not discriminate and, where possible, it promotes equality to meet the needs of the diverse patients and communities we serve.

This checklist is a way to help you think carefully about the likely impact on equality groups and take action to improve services. This is also an opportunity to evidence positive practices in our services and demonstrate strategic integrity to ensure that our services and employment practices are fair, accessible and appropriate for all patients, visitors and carers, as well as our talented and diverse workforce.

Name of the policy / function / service development being assessed	Patient and Staff Confidentiality Policy
Briefly describe its aims and objectives:	To inform staff about their legal duty to keep patient and staff information held in whatever form, confidential and secure.
Directorate and Lead:	IM&T Directorate – [redacted] (CIO) [redacted] (Head of IG and Coding)
Evidence sources: DH, legislation. JSNA, audits, patient and staff feedback	NHS Code of Practice: Confidentiality A guide to confidentiality in health and social care: Treating confidential information with respect Data Protection Act 1998, common law duty of confidentiality
Is the Trust Equality Statement present?	Yes

Equality Analysis Checklist

Go through each protected characteristic below and consider whether the policy, practice, function, business case, project or service change could have any impact on groups from the identified protected characteristic, involve service users where possible and get their opinion, use demographic / census data (available from public health and other sources), surveys (past or maybe carry one out), talk to staff in PALS and Complaints and Patient Experience. Please ensure any remedial actions are Specific, Measureable, Achievable, Realistic, and Timely (SMART).

Equality Group	Identify negative impacts	What evidence, engagement or audit has been used?	How will you address the issues identified?	Identifies who will lead the work for the changes required and when?	Please list positive impacts and existing support structures
Age	None identified	Passed by IG Group	N/A	N/A	The policy promotes equality by virtue of being neutral in all the listed categories.
Disability	None identified	Passed by IG Group	N/A	N/A	
Gender Reassignment	None identified	Passed by IG Group	N/A	N/A	
Marriage and Civil Partnership	None identified	Passed by IG Group	N/A	N/A	
Pregnancy and maternity	None identified	Passed by IG Group	N/A	N/A	
Race	None identified	Passed by IG Group	N/A	N/A	
Religion or Belief	None identified	Passed by IG Group	N/A	N/A	

Equality Group	Identify negative impacts	What evidence, engagement or audit has been used?	How will you address the issues identified?	Identifies who will lead the work for the changes required and when?	Please list positive impacts and existing support structures
Sex	None identified	Passed by IG Group	N/A	N/A	
Sexual Orientation	None identified	Passed by IG Group	N/A	N/A	
Carers	None identified	Passed by IG Group	N/A	N/A	

Equality Analysis completed by:	Organisation	Date
[redacted]	RFL	13-05-2014
IG Group	RFL	05-06-2014

Appendix K - Publication and Communication checklist

Title of document:	Patient and Staff Confidentiality Policy		
Date finalised:	23-05-2018	**Dissemination lead:** (print name and contact details)	[redacted]
Previous document already being used?	**Yes**		
If yes, in what format and where?	Electronic on freenet		
Proposed action to retrieve out-of-date copies of the document:	Remove out-dated policy from trust intranet		

To be disseminated to:	**How will it be disseminated, who will do it and when?**	**Paper or electronic**	**Comments**
Information Governance Group	Email, hand delivered group papers	Both	Approved IG group (chairmans action) 23.05.2018
Staff	Available on freenet – policies and procedures	Electronic	Policy will be available for intranet download

Date put on register / library of procedural documents	23/05/2018	**Date due to be reviewed**	01/04/2020