University Hospitals of Leicester NHS
NHS Trust

Personal Information Policy (Formerly Protection and use of Personal Information Policy)

Approved By:	Policy and Guideline Committee
Date of Original Approval:	12 November 2007
Trust Reference:	**B39/2007**
Version:	4
Supersedes:	3 – June 2020 Policy and Guideline Committee
Trust Lead:	Saiful Choudhury
Board Director Lead:	Andrew Carruthers – Chief Information Officer & Senior Information Risk Owner
Date of Latest Approval	21 January 2022 – Policy and Guideline Committee
Next Review Date:	May 2025

CONTENTS

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

Version	**Date**	**Author**	**Change**
4	December 2023	SC	• Check and update policies list. • Update names and roles in the policy • Clarification of bullet points 5 and 10 following review by PGC
3	January 2019	SC	• GDPR and new Policy Format incorporated
2.3	January 2009	GL	• Clarification following PGC comment.
2.2	December 2009	GL	• Clarification of points 10 and 13 following review by Medical Records
2.1	December 2009	GL	• Minor clarifications following standard review period
2	November 2007	GL	• Change to Policy status • Change in emphasis from patient information to personal information, ie to put emphasis more strongly on staff information. • Minor amendments and referencing • Amendments to reflect Staff Side input • Make explicit reference to smartcards
1	2002	AR	• Initial Staff Code of Conduct for the Protection and use of Patient Information. Agreed with the JSCNC and Trust Executive

KEY WORDS

Data Protection Act, GDPR, Information, Personal

1 INTRODUCTION AND OVERVIEW

This policy will set out the issues that staff need to be aware of when using patient and staff personal information and the responsibilities that staff have for maintaining the security and confidentiality of that information.

Patients expect that information about them will be treated as confidential and are given that assurance in the NHS Code of Confidentiality and the NHS Care Record Guarantee

2 POLICY SCOPE

This policy is applicable to permanent or temporary staff, students, volunteers, holders of honorary contracts and contractors.

3 DEFINITIONS AND ABBREVIATIONS

3.1 **Patient information** applies to all personal information known about a patient, whether this is manually recorded or held on computer. In addition to clinical information, the term also includes any non clinical information such as identification detail and hospital attendances.

3.2 **Identifiable data/information** relates to details from which the patient can be identified, for example Forename, Surname, Address, Postcode, Date of Birth, Other dates (i.e death / diagnosis), NHS/National Insurance or G.P Practice Number, gender or ethnic origin.

3.3 **Staff information** means details about permanent or temporary staff, students, volunteers, holders of honorary contracts and contractors which would not normally be public knowledge, for example home address, salary details, sickness records and so on.

4 ROLES AND RESPONSIBILITIES WITHIN THE ORGANISATION

4.1 **Senior Information Risk Officer (SIRO).** The UHL SIRO is the Chief Information Officer. The SIRO has the overall responsibility to ensure that any data that leaves the Trust has met the assured contractual process as well as the following:

Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers;

Owning the organisation’s overall Personal Information Policy and processes within and ensuring they are implemented consistently by information asset owners;

Advising the Chief Executive or the relevant accounting officer on the information risk aspects of the personal information being released if required;

4.2 The Caldicott Guardian

Has an “authorising” role, and facilitate any contract or clinical audit process where data is being released from the Trust after validation from the Trust Data Protection Officer. UHL Caldicott Guardian is the Medical Director.

4.3 Data Protection Officer/Head of Privacy

Develops the Personal Information standards for the Trust, based on NHS Digital guidance, gaining information on any security issues by networking with other Trusts, liaison with staff and industry best practice for personal information dissemination.

The Head of Privacy is responsible for the maintenance of this policy.

4.4 **Information Asset Owners** (i.e. those staff who have responsibility for specific projects or audits involving the release of personal data) will comply with the Trust policy and procedures which are defined in this policy and disseminate to the administrating colleagues who look after the data on a daily basis.

4.5 **Staff members** all have a responsibility for the security of personal information in electronic or manual systems. This includes:

Not sharing logins, passwords or smartcards;

Ensuring that personal data in electronic format on portable media is encrypted.

Members of staff who originate **new or revised flows of personal data** within and outside of the Trust are responsible for ensuring that information flow mapping is carried out, the information security risks of the data transfer are assessed (seeking advice from IM&T where appropriate).

5. Policy implementation and Associated Documents

All personal information, in any form whatsoever, must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it.

All employees of University Hospitals of Leicester are responsible for maintaining confidentiality of personal information

The duty of confidentiality is written into all employment contracts and is well established as common law meaning that personal information is confidential to the individual and should not generally be disclosed without consent unless justified for a lawful purpose (required by statute).

Clinical staff may legitimately use personal information for audit purposes. Research requires patient consent. For further information see the Data Protection Policy.

Breach of confidentiality of information gained, whether directly or indirectly, in the course of duty is a disciplinary offence, which could result in dismissal and/or prosecution.

5.1 When information may be disclosed

Information may be passed on to another party as long as the individuals are provided with adequate information regarding the possible uses of their information and the individuals consent is obtained, subject to Section 5 above. If consent is obtained, information can only be discussed in accordance with the terms of the consent given.

You are responsible for ensuring that patient and personal information is only used for specified and lawful purposes, that you respect medical confidentiality and that you understand and comply with the law. If at any time you are unsure whether to pass on any information, you must seek advice from your line manager, another more senior member of staff or from any of the contacts listed at the end of this document

5.2 Passing on information without consent

It may sometimes be necessary to pass on information without consent, for example:

In order to protect children or safeguard a vulnerable adult from significant harm

In order to protect the vital interest of the patient / client

In order to prevent or detect, or to support prosecution in respect of serious arrestable offence

Where required by Statute or Court Order

The decision in circumstances such as these, where no Trust Policy exists or where there is uncertainty over disclosure can only be made with approval of the Corporate and Legal Affairs Directorate through the Head of Legal Services or the Head of Privacy and / or the Trust's Patient Records Service Manager.

5.3 Public interest disclosure

Passing on information can in some instances be justified for other reasons, for instance to protect public interest. Where relevant this should always be done in line with the Trust's Freedom to Speak up: Raising Concerns (Whistleblowing) Policy, copies of which are available on Insite.

5.4 Password security and staff responsibilities

Data security will be protected against unauthorised access by the use of a combination of user identification (including smartcards) and individual password controls.

Staff are responsible for not sharing passwords, logins and smartcards and for logging off, removing smartcards or closing down terminals when they move away, thus preventing others from using the staff members login details.

It is the duty of all data users to comply with the Data Protection Act 2018, General Data Protection Regulations (GDPR) and Computer Misuse Act 1990

See Appendix 1.

To ensure compliance, computer activity including the use of the Internet and e-mail services, may be monitored. Any breach of confidentiality of information gained, whether directly or indirectly in the course of duty is a disciplinary offence which could result in dismissal or termination of agreement and/or prosecution.

The trust's information security and data protection policy and other guidelines which state the Trust's policy and procedures for maintaining confidentially of patient and personal information are available on Insite.

5.5 Summary of responsibilities

You are responsible for ensuring that:

5.5.1 Personal information obtained directly or indirectly during the course of duty is not disclosed to any person, organisation or body who does not need to know or who does not have an authorised right of access to that information. This includes staff not directly involved in the care of a patient

5.5.2 Every use or transfer of patient identifiable information must be clearly defined and justified. Wherever possible information should be anonymised. Do not use patient identifiable information unless it is absolutely necessary and only then use the minimum amount of identifiable information e.g. hospital number instead of name.

5.5.3 All information recorded must be, to the best of your knowledge, accurate and up to date. A data user must not wilfully record inaccurate data. Neither should you attempt to update or modify information that you are not authorised to update or modify

5.5.4 You must not divulge your security passwords to any other person. If you suspect that you password is known then it is your responsibility to change your password immediately and report the security breach to the IM&T Service Desk on x8000.

5.5.5 You must not use another persons' password, login or smartcard to gain access to information, even if you are authorised to have access. Neither must you attempt to gain access to any part of the system or information that your access privileges do not allow. Staff are to remove their smart card (if used)

5.5.6 You must not leave a terminal that is logged onto the system unattended. You are responsible for either terminating the session when finished or locking the screen if leaving the terminal unattended for even a brief period.

5.5.7 Health or staff records should not be left unattended in public areas and should be protected against loss, damage or unauthorised disclosure at all times. Printed material containing identification information should not be left unattended on printers or photocopiers.

5.5.8 You must not extract or download patient identifiable information from the hospital systems onto another computer system without permission from either the Trust's Caldicott Guardian or the Information Governance Manager

5.5.9 All personal information must be kept separate from general departmental waste and confidentially shredded.

5.5.10 Do not access information about yourself via clinical systems as you do not have an automatic right to such information - access requests for medical records must be made to your Consultant during an appointment or inpatient stay or to the Access to Health Records Department. Access to personnel files should be requested via your line manager.

5.5.11 You must not access information about relatives, friends or anyone else, even if they ask you to, unless you are required to do so as part of your job within the Trust. To do so is an offence under the Data Protection Act.

5.5.12 Do not give confidential information over the telephone without first checking the identity and authority of the caller/receiver

5.5.13 Do not send patient case notes via the internal postal system without first sealing them in an envelope and ensuring that the address is correct and clearly written. Do not send patient cases notes outside the Trust using Royal Mail. Any notes that need sending out of the Trust should go via Medical Records who will ensure that the notes are sent recorded or special delivery as appropriate. Contact Medical Records for further advice. In cases of Claims, Inquests or Police Investigations then the Claims and Inquest Team shall be authorised to send medical records outside of the Trust and when doing so they shall ensure that the notes are sent recorded delivery or special delivery as appropriate.

5.5.14 Every member of staff has the right to ask for proof of identity before passing confidential information on.

5.5.15 Personal data held on disk, CD, memory sticks or other portable device or media must be encrypted.. Consult the Service Desk (x8000) for details on encryption.

5.5.16 Personal data must not be emailed externally or sent over the internet unless it is encrypted or within a secure system

5.5.17 Do not hesitate to seek advice from any of the contacts named within this document should you feel that you need additional guidance.

5.6 Breaches of confidentiality

Patients

Patients who feel that confidence has been breached may raise the issue with any member of staff or issue a complaint under the NHS complaints procedure.

Breaches may also be reported to:- The Privacy Unit via infogov@uhl-tr.nhs.uk

The matter should be formally raised as complaint or an incident depending upon the circumstances of the breach. Major confidentiality breaches outside of hours should be escalated as any other incident.

Staff

Staff who feel their confidence has been breached may complain to their line manager, and request that the complaint be investigated as a formal grievance or complaint under the UHL Staff Complaints, Grievance and Disputes (Differences) Procedures.

5.7 Raising the matter outside of the Trust.

Patients and staff who consider the Trust has handled their personal data inappropriately could ask the Information Commissioner for an assessment of the Trusts practices. Patients or staff could also take legal action if the breach of confidence caused substantial damage or distress.

Should you require any further details regarding interpretation of this policy or If you have any queries or concerns you should contact your line manager or any one of the above individuals.

5.8 Monitoring breaches of confidentiality

Incidents and complaints will be reviewed and reported to the Information Governance Steering Committee

6 EDUCATION AND TRAINING REQUIREMENTS

All colleagues must take the mandatory course on Cyber Security and Data Protection Training available on the Trust Health Education & Learning Management (HELM) tool which also forms part of the Trust induction training.

7 PROCESS FOR MONITORING COMPLIANCE

Element to be monitored	**Lead**	**Tool**	**Frequency**	**Reporting arrangements Who or what committee will the completed report go to.**
Incidents and Data breaches	Head of Privacy	Breach Register	Every 3 months	IG Steering Group

8 EQUALITY IMPACT ASSESSMENT

8.1 The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

8.2 As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

9 SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

Policy
Email and Internet Usage Policy A9/2003
Freedom to Speak up: Raising Concerns (Whistleblowing) Policy A15/2001
Information Security Policy A10/2003
Data Protection and Confidentiality Policy A6/2003
Resolution Policy and Procedure B39/2020
Safeguarding Audlts Policy B26/2011
Safeguarding Children Policy B1/2012

10 PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

10.1 This policy will be reviewed every three years (or sooner if new legislation, codes of practice or national standards are to be introduced). The Policy and Guideline Committee is responsible for reviewing and approving policies.

10.2 The updated version of the Policy will then be uploaded and available through INsite Documents and the Trust's externally-accessible Freedom of Information publication scheme. It will be archived through the Trust's PAGL system