Oxford University Hospitals
NHS Foundation Trust

Information Protection Policy

Category	Policy
Summary	Main policy document for information protection
Equality impact assessment	February 2015. Reviewed June 2023
Valid from	Once approved
Date of next review	July 2026
Approval date	3rd August 2023 at Trust Medical Executive (TME)
Distribution	All staff
Related documents	Component policies as listed on page 2.
Author	Dr C Bunch, Data Protection Officer
Further information	
This document replaces:	Information Protection Policy v5.5 (July 2020)

Lead Director: Chief Digital and Partnership Officer

Issue Date: 03/08/2023

This document is uncontrolled once printed.

It is the responsibility of all users to this document to ensure that the correct and most current version is being used.
This document contains hyperlinks to other related documents.
All users must check these documents are in date and have been ratified appropriately prior to use.

Who should read this policy?

1. These policies are concerned with the integrity and security of personal data (patients, staff and others) and with the protection of privacy and confidentiality where appropriate. They are required for compliance with the Data Protection Act (2018), the UK GDPR, and the annual NHS Data Security and Protection Toolkit.

Background/Scope

2. Updates previous versions of the policy suite.
3. Applies to all staff (substantive & honorary) and external contractors.

Key Updates.

4. General updates to keep up with national requirements.

Aim

5. Compliance with national and legal requirements.

Content of the Policy

6. This Policy document comprises this document and the attached component policies, which are also available separately:

Acceptable use policy: the responsibilities of users with respect to IM&T/Digital Services including internet use, email and social media
Network security policy: how the OUH networks and nformation technology (IT) infrastructure will be kept secure
Mobile devices policy: governing the use of portable IT equipment
Safe haven policy: covers the arrangements and procedures necessary to ensure the safe receipt and storage of confidential information.
Pseudonymisation and anonymisation: Policy and Procedures: the GDPR and Caldicott Principles advise that personal data be de-identified where possible.
Clear Desk and Screen Policy: keep your workspace clear to protect sensitive information from prying eyes.
Photography and video policy & guidelines: governs the acquisition, storage and transmission of clinical images.
Registration authority policy: issuing and use of smartcards to authenticate access to NHS systems.
Information security policy for third-party suppliers: Most major NHS data breaches occur in systems supplied by third parties.

Review

7. This policy will be reviewed at least every 3 years and may be amended at any time to reflect changing circumstances and national requirements. Component policies may be updated at any time to maintain compatibility with the changing NHS information security landscaoe.

References

8. Data Protection Act (2018) as updated June 2023 (includes the UK GDPR).

Document History

Date of revision	Version number	Author(s)	Reason for review or update
Aug 2023	5.6	Dr C Bunch Data Protection Officer	Approved by TME 03/08/2023
Jun 2023	5.6d	Dr C Bunch Data Protection Officer	General update. New format
Jul 2020	5.5	Dr C Bunch Data Protection Officer	General update.
Nov 2018	5.4	Dr C Bunch Caldicott Guardian Nuala Buchan Brodie IG Manager	Minor updates and corrections and to include pseudonymisation and clear desk policies
Feb 2018	5.3	Dr C Bunch Caldicott Guardian	Alignment with Data Protection Act 2018
Nov 2016	5.2	Dr C Bunch Caldicott Guardian	Updated to include safe haven policy
Nov 2015	5.1	Dr C Bunch Caldicott Guardian	Updated to include confidentiality policy (later moved to IG Policy)
Feb 2015	5.0	Dr C Bunch Caldicott Guardian Phil Pinney IM&T	Extensively updated to incorporate IM&T security policies

Consultation schedule

Who? Individuals or Committees	Method of involvement
Shared with Divisional Directors and Directors of Operations and key Digital staff	Via email

Endorsement

Chief Digital and Partnership Officer (CDPO)

Appendix 1: Responsibilities

1. The Chief Executive, as the Accountable Officer, has overall responsibility for information governance and data protection and is required to provide assurance through the Statement of Internal Control that all risks to the Trust are effectively managed and mitigated.
2. The Senior Information Risk Owner (SIRO), has delegated responsibility for ensuring that effective systems and procedures are in place to ensure implementation of this policy.
3. The Caldicott Guardian is responsible for overseeing and advising on processes to satisfy the highest standards for handling personal identifiable information.
4. The Data Protection Officer independently advises on and monitors the Trust's data processing activities and data security.
5. The Information Governance Manager is responsible for supporting and monitoring the implementation of this policy.
6. Managers are responsible for ensuring that:
    - all staff, including temporary staff, contractors and volunteers, understand and accept what is expected of them with respect to confidentiality and protecting information;
    - staff for whom they are responsible have the appropriate information governance training for their role.
7. Individual staff members are responsible for:
    - complying with this policy and its component parts;
    - safeguarding the confidentiality of all personal and Trust information, transmitted or recorded by any means;
    - reporting any incidents or near misses where information breaches have or could occur.

Appendix 2: Definitions

1. The terms in use in this and component documents are defined as follows:

- *Senior Information Risk Owner (SIRO)* – the Trust SIRO is responsible for ensuring information risk is properly identified and managed, and that appropriate assurance mechanisms exist;
- *Caldicott Guardian* — a senior individual who ensures that personal information is used legally, ethically and appropriately, and that confidentiality is maintained;
- *Information asset* – a digital or paper-based repository of information.
- *Information asset owner (IAO)* – the senior individual responsible for managing an information asset;
- *Information asset administrator (IAA)* – the day-to-day system managers of an information asset, usually responsible for security, access, backups and user management;
- *System Level Security Policy (SLSP)* – A document used to register an information asset which describes ownership, management, processing, storage, risk, access, retention, transfers of data, business continuity, recovery of the data on that system;
- *Personal or person-Identifiable Data (PID)* – data or information from which can be identify an individual or individuals either on its own or if combined with other information which is in the possession of, or is likely to come into the possession of the holder of the information;
- *Processing* – in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

  (a) organisation, adaptation or alteration of the information or data,
  (b) retrieval, consultation or use of the information or data,
  (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
  (d) alignment, combination, blocking, erasure or destruction of the information or data;

- *Data Controller* – a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;
- *Data Processor* – in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Appendix 3: Education and Training

8. All staff must undertake annual data security and protection training for compliance with the NHS Data Security and Protection Toolkit. Management and monitoring of training will be in accordance with the OUH Learning and Development Policy. Information on this can be accessed via the Practice Development and Education pages on the Trust intranet.

Appendix 4: Monitoring compliance

Compliance with this policy will be monitored in the following ways.

What is being monitored:	How is it monitored:	By who, and when:	Minimum standard	Reporting to:
Policy implementation and staff compliance	Monitoring and investigation of training and information - related incidents	Information Governance Team. Divisional Directors of Operations. Monthly	95% compliance	Digital Oversight Committee Data Protection Officer
Policy implementation and staff compliance	Spot checks of departmental areas and audits	Information Governance Team.	95% compliance	Digital Oversight Committee Data Protection Officer

Appendix 5: Equality Impact Assessment

Equality assessment: Information Governance Policy
June 2023
Review date: *June 2027*
Does the policy /proposal relate to people? *Yes.*
Identify the main aim and objectives and intended outcomes of the policy. *This policy is intended to ensure appropriate governance of information held by the Trust.*
Involvement of stakeholders *The policy has been developed by the Senior Information Risk Officer, Caldicott Guardian, Information Governance Team, and the Data Protection Officer. It takes into account feedback from incidents, complaints, advice and guidancefrom the Information Commissioners Office and others.*
Evidence
Disability Have you consulted with people who has a physical or sensory impairment? How will this policy affect people who have a disability? *No. Not relevant.*
Sex How will the policy affect people of different gender? *Equally*
Age How will the policy affect people of different ages – the young and very old? *Equally*
Race How will the policy affect people who have different racial heritage? *Equally*
Sexual orientation How will the policy affect people of different sexual orientation- gay, straight, lesbian, bi-sexual? *Equally*
Pregnancy and maternity How will the policy affect people who are pregnant or with maternity rights? *Equally*
Religion or belief How will the policy affect people of different religions or belief – or no faith? *Equally*
Gender re-assignment How will the policy affect people who are going through transition or have transitioned? *Equally*
Marriage or civil partnerships How will the policy affect people of different marital or partnership status? *Equally*
Carers Remember to ensure carers are fully involved, informed, supported and they can express their concerns. Consider the need for flexible working. How will carers be affected by the policy? *n/a*
Safeguarding people who are vulnerable: How has this policy plan or proposal ensured that the organisation is safeguarding vulnerable people? (e.g. by providing communication aids or assistance in any other way.) *Safeguarding information relating to vulnerable people is an integral part of this policy.*
Other potential impacts e.g. culture, human rights, socio economic e.g. homeless people *n/a*
Summary of analysis Does the evidence show any potential to discriminate? *No. All staff and contractors are equally bound by this policy.*

Acceptable Use Policy

Introduction

1. Oxford University Hospitals NHS Foundation Trust (OUH) provides network and computing resources to support its primary function of patient care. To ensure the availability of these resources, and the safe and secure use of information which may be confidential and/or sensitive, users have responsibilities which are described in this document.
2. Access to and use of OUH's information systems is logged and regularly monitored. Misuse of these resources constituting a breach or disregard of this policy may lead to disciplinary action up to and including dismissal.
3. This document is a component of the OUH Information Protection Policy and should be read in conjunction with the parent policy and its other components.

Scope

4. For the purposes of this Policy, the terms "*network*", "*computing*", "*resources" and "services"* together or in combination refer to any of the available OUH Digital resources, including any of the network-borne services, applications or software products, and the network/data transport infrastructure used to access any of the services (including access to the internet).
5. The term *session* in this Policy refers to a specific connection made by a user to a system by logging in with a username and password.
6. Individuals covered by this Policy include anyone (staff, students, contractors, etc.) using or having access to the Trust's computing resources, hereinafter referred to as *Users*.

Policy

7. Users must at all times:
    - comply with the law;
    - comply with all OUH and system-specific policies and procedures for the operation and/or use of the resources;
    - use or access only those equipment, services programs, information or data, for which they have specific authorisation;
    - ensure that passwords and digital resources to which they are responsible are protected from unauthorized use or access;
    - use only those usernames and passwords that have been issued to them personally for logging into OUH systems;
    - respect the privacy and personal rights of data subjects (e.g. patients) and other users;

- respect OUH's good name and reputation of in all internal and external communications.

8. Users must **not:**
   - interfere with others' use of the resources;
   - use any of the resources to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person;
   - use any of the resources for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such;
   - attempt to access restricted portions of the network, any operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator;
   - access or attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator;
   - use programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system;
   - use the resources for any form of commercial activity (including private medical practice) without express permission;
   - use the resources for any form of mass, unsolicited mailings (i.e. spam);
   - install, use or distribute software without an appropriate licence.
9. In addition to these general rules, users must comply with the following requirements.

Patient (clinical) systems

10. Users may only access records of patients with whom they have a legitimate relationship, normally those for whom they have direct clinical responsibility. Some systems, e.g. the electronic patient record (EPR), require users formally to confirm their relationship to the patient. This action is logged and monitored. Users are not permitted to access their own records directly: these may be only viewed through a formal subject access request (see the Information Governance Policy: Subject Access Requests).
11. Users may only access patient records through sessions that they have personally logged into. Users **must not** share sessions with other users, or take over a session started by another user. Users wishing to use a terminal that already has a session running must terminate that session first before logging into a session of their own. This applies to all forms of session, whether initiated by smartcard or username/password entry.

Passwords

12. Passwords are issued to (or created by) users for their own, personal use only and must **never** be shared with anyone else. Shared access to some services such as email is possible but must be configured in the system by the sharing user and not achieved by sharing passwords.
13. Users should follow OUH guidance when choosing a password. A separate, unique password should be used for each application or resource that requires a password.
14. Passwords must be kept secure at all times. **Never** write them down and leave them where others can find them.

Smartcards

15. OUH staff are issued with NHS smartcards which contain a near-field communication (NFC) chip pre-programmed with user credentials, together with a password. This combination allows two-factor authentication—something you have (a smartcard) and something only you know (a password— which is required for access to systems that access the NHS Spine Services. Smartcards are used principally by clerical staff to access the EPR and electronic referral systems —where access to the Spine demographics is required —and by clinical staff accessing the network using the 'tap-and-go' system (see below).
16. Staff must **never** leave their smartcard in the computer slot unattended, nor allow anyone else to use their smartcard. Loss of a smartcard must be reported to the issuing (Registration Authority) office *and* reported on Ulysses.
17. Smartcards are also used for 'tap-and-go'--a network access method in which users create or gain access to a session they have previously created, by tapping a near-field detector attached to an enabled workstation. The user will be required to enter his/her active directory username and password unless this has been recently entered to the network. This is used to ensure that the smartcard belongs to the user.
18. Sessions created by tap-and-go must always be closed before leaving the workstation, by tapping with the smartcard once again. The server retains the current state of the session which can be retrieved by tapping again at the same or a different workstation.

Email

19. OUH provides an email service for its employed and honorary staff (addresses with the format *user.name@ouh.nhs.uk*). This is the primary service for communication within OUH and staff are expected to monitor their accounts regularly. Some staff may also have accounts with the NHS Mail email system (addresses with the format *username@nhs.net*). Staff must only use ouh.nhs.uk or nhs.net for OUH business (i.e. **must not** use any other email system).
20. Email messages have the same legal status as written correspondence. Staff using email must abide by this policy and follow the accompanying guidelines, and are responsible for using email safely and legally, and where appropriate maintaining confidentiality.

21. Remember that any message content that identifies an individual person will be disclosed to that individual if the make a subject access request under the UK General Data Protection Regulation (GDPR).
22. Email should not be considered as a fully-secure medium. Whilst messages are transmitted securely, users are responsible for ensuring correct addressing and appropriate content. Most confidentiality breaches by email occur because of incorrect addressing. Take especial care when forwarding or replying to messages.
23. Confidentiality breaches may be avoided by:
    - checking that you have the recipient's correct email address;
    - taking care when entering the address(s) into the email form. Outlook remembers who you have emailed in the past and it is possible to select the wrong recipient with the same or similar name;
    - when possible, only send to one recipient at a time. Avoid sending to group addresses;
    - if sending a confidential message to more than one recipient, put their addresses into the Bcc: field, not the To: or cc: field. This will avoid addresses being visible to recipients .
24. Messages must not include patient or person-identifiable information (PID) unless strictly necessary and justifiable (Caldicott Principles 1,2 & 3). Copies of any messages that have clinical information relevant to a patient's care **must** be filed in the patient's EPR record
25. Messages may be sent direct to patients' personal email accounts from OUH or NHS Mail accounts with the patient's permission and understanding that transmission is not necessarily secure. Where secure transmission is required, OUH staff can use Office 365 Message Encryption (OME) to encrypt their messages and attachments. Recipients will be able to read the message once they have authenticated and signed into their email provider.
26. Messages containing patient-identifiable information must otherwise **not** be transmitted by any other email system or sent to addresses at other email systems.
27. When receiving messages, always be suspicious of potentially harmful content, especially if from an unknown sender. To protect yourself and OUH you must:
    - never open attachments or links from unknown or un-verified sources;
    - never divulge sensitive information such as passwords or personal details. If in doubt, find the sender's telephone number from a legitimate source and contact them to verify the request;
    - be aware that criminals often use social engineering techniques appear legitimate or trustworthy;
    - never open or respond to suspicious emails. Responding lets the sender know that the address is valid and may lead to further spam messages to that address.

- be cautious when disclosing email addresses to non–NHS sources to reduce the likelihood of receiving spam.

28. If you have any doubts or concerns about a message received, contact the IT Service Desk immediately for advice.
29. You may make limited use of OUH email for purposes not related to work provided that:
    - it does not interfere with their work;
    - it is not related to a private business interest or to employment with another employer'
    - it is not used for personal commercial purposes;
    - it complies with OUH policies.
30. Messages concerning OUH business and activities must reside on the OUH server and must not be downloaded and stored on client devices.
31. Messages should be deleted as soon as they are no longer required unless they are (or may reasonably expected to be) relevant or involved in a subject access or freedom of information request. (See the *NHS Records Management Code of Practice 2021* pp. 109–110.)
32. All email messages handled by the OUH email system, together with emails created by staff on OUH business that are transmitted through other email systems (including NHS Mail) are the property of OUH. They subject to the provisions of the Data Protection Act for subject access requests, and the Freedom of Information Act. OUH Digital staff may inspect any user's mailbox at any time for security reasons or to investigate possible breaches of this policy.

Internet use

33. Access to the public internet is provided for business use to support patient care, education, training, and research, and to access information relevant to users' work.
34. The internet may be used for access to resources for personal use provided this does not interfere with the user's work or OUH business, and are compliant with other clauses of this policy.
35. The OUH Information Protection Policies apply equally to the use of the internet.
36. The following activities, or visiting sites conducting such activities, are expressly forbidden:
    - any illegal purpose or the display or downloading of any illegal or pornographic material;
    - gambling;
    - discrimination, harassment, disseminating libellous statements;
    - share trading or money-making schemes;
    - breaching confidentiality and/or publishing patient-identifiable data;

- copyright infringement;
- multimedia or music downloads (unless for work purposes);
- viewing or downloading offensive material, as defined by the OUH Equal Opportunity and Harassment Policy. This includes hostile text or images relating to gender, ethnicity, race, sexual orientation, religious or political convictions and disability.

37. This list is not exhaustive. Other than instances which demand criminal prosecution, the Trust is the final arbiter on what constitutes offensive material, and what is or is not permissible internet access.

38. Users should be aware that their access to the internet is logged, monitored, and audited. Misuse will be reported to the user's manager and may result in disciplinary action.

Document History

Version	Date	Author(s)	Comment
1.6	August 2023	Dr Chris Bunch Data Protection Officer	Approved by TME 03/08/2023
1.6.1d	July 2023	Dr Chris Bunch Data Protection Officer	Clause 24 amended
1.6d	June 2023	Dr Chris Bunch Data Protection Officer	Password section updated.
1.5	March 2023	Dr Chris Bunch Data Protection Officer	General update for compliance with DCB1596 (Secure email).Approved by DOC May 2023
1.4	December 2018	Dr Chris Bunch Caldicott Guardian	Minor amendments to email section
1.3	June 2018	Dr Chris Bunch Caldicott Guardian	Clarification regarding emails to patients
1.2	February 2018	Dr Chris Bunch Caldicott Guardian	Updated for Data Protection Act 2018
1.1	September 2015	Dr Chris Bunch Caldicott Guardian	Email section updated regarding local storage of emails (para 27)
1.0	March 2015	Dr Chris Bunch Caldicott Guardian	Created as a component policy document of the Information Protection Policy

Network Security Policy

Introduction

1. Oxford University Hospitals NHS Foundation Trust (OUH) relies heavily on information technology (IT) to support its activities, and the security of its IT systems is paramount. Systems must be available when required, reliable, and safe. As the OUH's main activity is the clinical care of patients, it is of particular importance that the confidentiality and security of patient information collected and stored on OUH systems is maintained. This policy document sets out the actions and responsibilities required to achieve these aims.
2. OUH Digital Services (IM&T) will ensure that the network is available when needed, can be accessed only by legitimate users, and be able to withstand or recover from threats to its availability, integrity and the confidentiality of information therein (cyber security). It will achieve this by:
    - protecting all hardware, software and information assets under its control through the implementation of a set of well-balanced technical and organisational measures;
    - undertaking regular cyber security risk-assessments covering all aspects of the network that support the OUH's business processes, and reporting these to the Trust Board;
    - providing protection that is effective, cost-effective, and commensurate with the assessed risks to its network assets;
    - implementing a robust cyber security programme of appropriate technical processes, controls, staff awareness and training required to comply with the NHS Data Security and Protection Toolkit standards.
3. This document is a component of the OUH Information Protection Policy and should be read in conjunction with the parent policy and its other components.

Scope

4. For the purposes of this policy, the network comprises the totality of OUH's computing and communication equipment such as servers, computers, printers, routers and switches, that are connected together by cables or wireless, and the data contained or transmitted therein.
5. The scope includes mobile devices, such as laptops and mobile phones, whether provided by OUH or personally-owned if they are used for OUH business and/or communicate with the OUH networks. (See also the Mobile Devices policy.)
6. This policy applies to all electronic data systems used for OUH's clinical and non-clinical activities, whether or not directly managed by OUH Digital Services.
7. It applies also to the provision of access to the internet and the Health and Social Care Network (HSCN) or any future replacement, "cloud computing services", and to all forms of remote access to OUH's networks and systems.

Responsibilities

8. The overall responsibility for information security rests with the Senior Information Risk Officer (SIRO) who has formally-delegated authority from the Chief Executive Officer. Day-to-day responsibility for the security of the physical IT infrastructure is delegated through the Director of Digital Services to the Head of IT.
9. Each significant component of the network, as defined above, is considered to be an information asset and as such must be assigned an information asset owner (IAO) and manager (IAM) as defined in the OUH Information Governance Framework. The OUH Information Asset Register must be updated for each asset.
10. Responsibilities of the Senior Information Risk Officer, Information Asset Owners and Information Asset Managers are as defined in the Information Governance Framework component of the Information Governance Policy.
11. Systems that are part of the network as defined above, but which are not owned or directly managed by Digital Services, are the responsibility of the relevant Divisional Directors of Operations who must ensure compliance with this and other relevant policies as they apply to those systems. Such systems include, *inter alia,* laboratory and radiology information systems.

User responsibilities

12. The responsibilities of users of OUH's networks and systems are set out under 'User access' below, in the Acceptable Use Policy, and in specific system-related policies. All users must adhere to these requirements: failure to do so may lead to disciplinary action up to and including dismissal.

Physical & environmental security

13. Network equipment will be housed in controlled and secure environments. Critical or sensitive equipment will be housed in an environment that is continuously monitored for temperature, humidity and power supply quality, and will be protected from power supply failures, fire (with fire suppression systems as appropriate, and physical intrusion (using intruder alarms).
14. Smoking is forbidden on all OUH premises. Food and drink must not be taken into areas housing critical or sensitive network equipment.

Access to equipment

15. Physical access to network equipment must be strictly controlled and monitored at all times.
16. Where possible equipment room access should be controlled using the ID card access system which records the time and the individual's identity for all accesses. Where this is not possible or practicable access doors must be secured with a high-security code lock. Responsibility for ensuring that door lock codes are changed periodically rests with the Director of Digital Services. In the event a key code is thought to have been compromised it must be changed immediately.

17. Entry to secure areas housing critical or sensitive network equipment is restricted to those who require access to carry out their jobs. Digital Services will maintain a list of staff members who are allowed unsupervised access and will ensure that areas controlled by ID cards are limited to registered individuals. Other persons requiring access must have a legitimate purpose and their access must be supervised and logged.
18. Visitors to secure network areas must be authorised by the Head of Infrastructure, and must be made aware of network security requirements and evacuation procedures. They must be accompanied by a responsible department member, and the purpose of visit, date, and time in and out must be logged.
19. The Data Centres at OCDEM and JR Level 0 have fire suppression systems which involve the release of dangerous gases. Nobody is allowed into these areas without first receiving training on the fire suppression system unless they are accompanied by Digital Services staff with the required training. Visitors are not allowed into these areas unaccompanied.
20. OUH has an agreement with Oxford Health Foundation Trust (OHFT) which allows OHFT designated space in the OCDEM Data Centre for its sole use. Designated OHFT IT staff have access to this facility at all times and have been provided with security swipe cards to facilitate secure and controlled access.

User access to the OUH network and systems

21. OUH staff may be granted network access depending on their job requirements and with the approval of their line manager. For some groups of staff (e.g. clinical staff) access will be granted to new staff automatically on starting. All users will be issued with a network username and password, and logins will be controlled via Active Directory. On first connection, users will be required to change their password and must choose a compliant password (see below). This process will be controlled and monitored by Digital Services, who will report any breaches or suspicious activity via the Ulysses incident reporting system.
22. All users must comply with the Acceptable Use Policy component of the Information Protection Policy.
23. Access to the network for staff on OUH premises will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. The procedure will be the same for access to wired and wireless networks.
24. Users must ensure that they protect the network from unauthorised access. Passwords must never be shared, and users must never take over (tailgate) a session someone else has left unattended.
25. Users must always log out of systems and/or the network when they have finished working and must never leave a live session unattended. Users finding an unattended session must always terminate the session before logging in with their own credentials.

26. The Resources department will notify all leavers to Digital Services, who will terminate their access.

Smartcards

27. OUH staff are issued with NHS smartcards which contain a near-field communication (NFC) chip pre-programmed with user credentials, together with a password. This combination allows two-factor authentication—something you have (a smartcard) and something only you know (a password)—which is required for access to the electronic patient record (EPR) and systems that access the NHS Spine Services such as the Summary Care Record (SCR). Smartcards are used principally by clerical staff to access the EPR and electronic referral systems—where access to the Spine demographics is required— and by clinical staff accessing the network.
28. Staff must never leave their smartcard in the computer slot unattended, nor allow anyone else to use their smartcard. Loss of a smartcard must be reported to the issuing (Registration Authority) office and reported on Ulysses.

Virtual workspace/desktop

29. Virtual workspace/desktop services are provided to connect users to the network and associated systems. Instead of logging into a local workstation and running local applications, the virtual application presents the user with a dedicated session that is running on a remote server, from which the user may access the services required. This improves security as no data is transmitted to or stored on the local computer. It is typically used with tap-and-go authentication (see below) and combined with a single-sign on facility that stores and enters users' passwords for available services to speed up access. Virtual sessions can be transferred intact between client computers, allowing the user to access their active session from any convenient networked computer.

Tap-and-go

30. Tap-and-go is a network access method in which a network user gains access by tapping a near- field detector attached to an enabled workstation. If the user has started an active virtual session on another workstation, this is retrieved and presented. Otherwise a new session is created.
31. The user will be required to enter his/her active directory username and password unless this has been recently entered to the network. This is used to ensure that the smartcard belongs to the user.

Wireless local-area networks (WLAN)

32. OUH provides two wireless networks: OxNET–WLAN is the secure corporate wireless network. Access is only available to staff members authorised by Digital Services and requires login using the standard Active Directory username and password. OxNET–WLAN is logically co-terminus with the corporate wired network and gives access to all networked services including the HSCN network and the internet.

33. An open network is also provided for 'guest' access by staff, patients and the public (OUH- GUEST). Users are required to enter their email address on connection and agree to the terms of the Acceptable Use policy. The network gives access to the internet though access to certain sites and services may be restricted or blocked by Digital services. It is possible to access OUH and NHS Mail email accounts, both directly and via a web browser, via this network.
34. All network logins will be logged. Digital Services will undertake periodic access audits and will investigate and report any inappropriate or suspicious events.

Connection of devices to the network

35. No device (PC, switch, hub, etc.) may be connected to the physical network (wired/wireless) without prior permission from Digital Services. Personal mobile devices (Apple and Android) must be registered via OUH Mobile Application Management (MAM). See also the Mobile Devices and Acceptable Use Policies.
36. Network login via Active Directory normally also grants users access to the networked device through which the user has connected. Security privileges (i.e. 'superuser' or local administrator rights) to specific devices may be granted according to the requirements of the user's job and at the discretion of Digital Services.
37. Users are not permitted to extend the network to other users by creating WiFi 'hotspots'.

Remote and third-party access

Virtual private network (VPN)

38. Users may be granted access to secure VPN access OUH network if appropriate to their job requirements and at the discretion of Digital Services. The security of VPN access is primarily the responsibility of Digital Services, and multi-factor authentication is required. Users should only access the VPN service from OUH devices or devices they own and have control over, and never from public computers.

Third party access

39. Third party access to the network may be granted for legitimate purposes such as system maintenance at the discretion of Digital Services and (where patient identifiable data may be accessed) the Caldicott Guardian. All such access must be based on a formal contract that satisfies all necessary NHS security conditions and has been agreed with Information Governance. For access to clinical systems, security vetting will be required.

Connection to external networks

40. Digital Services will ensure that all connections to external networks and systems have been documented on the OUH Information Asset Register. Digital Services will

ensure that all connections to external networks and systems conform to the NHS-wide Network Security Policy, Code of Connection and supporting guidance.

41. The Head of Infrastructure must approve all connections to external networks and systems before they commence operation.

Business continuity and disaster recovery

42. Digital Services will ensure that business continuity plans and disaster recovery plans for the network and connected systems for which they are responsible exist and are maintained. The plans must be reviewed and tested on a regular basis.
43. Digital Services is also responsible for ensuring that backup copies of network configuration data are taken regularly, stored securely, and available when required. Where operationally possible a copy will be stored off-site.
44. Documented procedures for the backup process and storage of backup media, and their safe and secure disposal, will be maintained by the Information Security Manager and communicated to all relevant staff.
45. Information asset owners are responsible for ensuring that appropriate backups of their systems are locally-managed and that business continuity plans and disaster recovery plans are produced and regularly tested. Critical, sensitive or confidential data must not be stored on unencrypted portable or removable devices (e.g. USB memory or hard disks).
46. Users are responsible for ensuring that their own data is backed up as required by storing their data on a secure network server that is regularly backed up.

Equipment procurement, deployment, maintenance and disposal

47. All network equipment and equipment connected to the network must be approved by Digital Services and must meet agreed security standards.
48. As part of acceptance testing of all new network systems, network managers will attempt to cause a security failure and document other criteria against which tests will be undertaken prior to formal acceptance. Where possible testing facilities will be used for all new network systems and development and operational facilities will be separated.

Maintenance

49. Digital Services is responsible for ensuring that maintenance contracts are maintained and periodically reviewed for all equipment.

Equipment re-use

50. Where possible equipment will be reallocated if it is fit for purpose and supportable, otherwise Digital Services will recommend that equipment reaching end-of-life be replaced.

51. Equipment to be replaced must have storage media removed, after which the equipment may be disposed of by through the Estates department. The removed storage media *must* be disposed of securely. Digital Services provides a service for the safe on-site destruction of media of all types and recording thereof. All storage media, both that removed from equipment or independent (e.g. backup tapes), should pass through this process.
52. The secure disposal of equipment not procured through Digital Services is the responsibility of the Information Asset Owner Any storage media should pass through the Digital Services media destruction process described in para. 52 above.

Security monitoring and incident reporting

53. Digital Services will ensure that the network is monitored for potential security breaches and that a log of all faults on the network is maintained and reviewed. All monitoring must comply with current legislation.
54. Digital Services will record any incidents in the Digital Services call management system. In addition, all potential security breaches will be reported via the OUH incident reporting system (Ulysses) and investigated. Serious incidents and weaknesses must be reported centrally via the Data Security and Protection Toolkit.
55. Incidents involving systems not managed by Digital Services must be reported by the relevant Information Asset Owner.

Document History

Version	Date	Author(s)	Comment
1.3	June 2023	Dr Chris Bunch Data Protection Officer	Approved by TME 03/08/2023
1.3d	June 2023	Dr Chris Bunch Data Protection Officer	Minor updates
1.2	May 2022	Dr Chris Bunch Data Protection Officer	Routine update
1.1	February 2018	Dr Chris Bunch Caldicott Guardian Phil Pinney Information Security Manager	Updated for the Data Protection Act 2018
1.0	March 2015	Dr Chris Bunch Caldicott Guardian Phil Pinney Information Security Manager	Created as a component policy document of the Information Protection Policy

Mobile Devices Policy

Introduction

1. This document establishes a standard set of requirements and a framework for the use and management of mobile devices for Oxford University Hospitals NHS Foundation Trust (OUH) business.
2. For the purposes of this policy, any reference to a mobile phone means smartphone, iPhone, Android, Windows or other mobile phone.
3. OUH uses Mobile Device Management and Mobile Application Management policies to set minimum standards for securely accessing OUH data from both OUH-owned and users' personally-owned devices.
4. Mobile Device Management helps to enforce a series of security requirements on mobile device themselves, such as password strength, operating system version, profile separation, encryption, data access and remote management.
5. Mobile Application Management helps to ensure that OUH data is only accessed from secure 'managed' applications which limit how data can be opened, copied and shared.
6. This document is a component of the OUH Information Protection policy and should be read in conjunction with the parent policy and its components.

Scope

7. The policy applies to the following classes of device:
    - smartphones (e.g., iPhone, Android phones, Windows phones);
    - tablets (e.g., iPad, Android, Windows tablets);
    - laptops/portable computers;
    - portable memory devices (USB sticks and external hard drives/SSDs).
8. The policy covers both OUH and user-owned devices used for OUH activities/business.
9. The policy applies to all staff (permanent, temporary, honorary) and to external contractors and anyone else using mobile devices for OUH purposes.

Criteria for the issue of a mobile device by OUH

10. An employee may be eligible to have a mobile device issued by OUH if it is deemed necessary to their position or function and they do not have or wish to use their own private mobile phone. Eligibility is at the discretion of the employee's Division. Digital Services will advise on the process for application and procurement via the Service Desk.

Use of personally-owned (BYOD[1]) devices

11. Staff are permitted to use their own devices on OUH premises provided that this does not interfere with the user's job or other staff's work, and subject to the conditions of this policy and the Information Protection: Acceptable Use Policy.
12. The device owner *must*, as a minimum, register the device into the OUH Mobile Application Management system. They may also choose to enrol their personally-owned device into OUH Mobile Device Management thereby increasing the protection applied to it.
13. Personally-owned devices:
    - may only connect to the OUH-Guest network i unless there is a genuine operational need to access a different OUH network;
    - must comply with the minimum version requirements are defined by the OUH Mobile Device Management;
    - must have OUH-approved anti-virus software installed and active.
14. Users must:
    - ensure that any component of the device (e.g. charger) that is connected to the OUH mains electricity supply has been checked for electrical safety in line with the relevant policy;
    - comply with all OUH Information Governance, Information Protection, and Digital policies. Misuse of a mobile device connected to OUH networks will result in disciplinary action being taken and possibly confiscation of the device.

Mobile phones — safety issues

15. Staff must only use their phone when it is safe to do so. Since December 2003, it has been an offence to use a hand-held phone when driving. Doing so may incur a fixed penalty: no such penalty charges will be reimbursed by OUH.
16. Using a mobile phone 'hands free' may also result in a fine and penalty points. Police can still use existing legislation (for failing to have proper control of the vehicle) if a driver is distracted by a call on a hands-free phone. If there is an incident and the driver is using any phone (hand-held or hands-free) or similar device, then there is a risk of prosecution for careless or dangerous driving.
17. To ensure compliance with legislation and to ensure personal safety and that of other road users, staff should either switch off their phone or use voicemail or divert calls whist driving.
18. OUH will accept no liability for the consequences of using a mobile phone (OUH or user- owned) whilst driving.

[1] 'Bring your Own Device' (BYOD).

Security of mobile devices

Physical security

19. Mobile devices are frequently and easily stolen and must not be left lying around or in view in an unattended vehicle. When not in use or being carried by the user, devices must be stored securely: preferably out of sight in a locked container in a locked room.

20. Loss or theft of any mobile device that connects to the OUH networks must, in the first instance, be reported to Digital Services (who will take action to locate and/or wipe the device remotely), and a Ulysses incident form completed. For phones, the network service operator should also be informed.

21. It is the user's responsibility to ensure that important data stored on the device is backed up elsewhere to ensure it is retrievable should a remote wipe be necessary.

Encryption

22. Mobile devices used to store person-identifiable data must be encrypted to the NHS standard, using AES256 with 256 bit or stronger keys. Encryption is enforced when devices are enrolled into OUH MDM, or registered into OUH MAM

23. Encryption keys or access codes must be kept safe and secure. If there is any doubt about the subsequent ability to gain access to the encrypted data in extreme emergencies, Digital Services can also store securely the key or access code.

Passwords

24. Devices that store or can access personal or sensitive information must be secured with a password that is known only to the owner and not shared with anyone. For devices that are shared between different users there must be separate accounts/profiles for each user, each with its own password.

Cloud services

25. File storage in 'the cloud' is increasingly popular as a means of synchronizing data between data devices and for backup. OUH data should only be stored in OneDrive for Business (Microsoft), or in an OUH-approved Electronic Patient Record.

Portable storage devices

26. Only devices encrypted to NHS standards may be connected or attached to computers that hold patient information or are connected to the OUH corporate network. This applies to USB flash drives and external hard drives. In exceptional circumstances unencrypted USB flash drive may be connected to computers that are never used to store or access patient information, for example to upload a presentation. Computers suitable for such purposes must be vetted and registered with the Information Governance team.

Document History

Version	Date	Author(s)	Comment
2.0	May 2023	Ralph Shakell, Information Governance Manager Dr Chris Bunch Data Protection Officer	Approved by TME 03/08/2023
2.0d	May 2023	Ralph Shakell, Information Governance Manager Dr Chris Bunch Data Protection Officer	Approved by Digital Oversight Committee
1.4d	Sept 2022	As below + Will Smith, Lucas Daka, Caleb Grant	Includes MDM/ MAM policies for DCB1596
1.3d	May 2022	Dr Chris Bunch Data Protection Officer	Updated for DCB1596 compliance
1.2d	February 2018	Dr Chris Bunch Caldicott Guardian	Updated for Data Protection Act 2018
1.1	July 2016	Dr Chris Bunch Caldicott Guardian	Minor corrections
1.0	March 2015	Dr Chris Bunch Caldicott Guardian	Created as a component policy of the Information Protection Policy

Safe Haven Policy and Procedures

Introduction

1. NHS organisations are required to have policies and procedures to ensure the safe and confidential handling of personal information.
2. This policy document covers the arrangements and procedures necessary to ensure the safe receipt and storage of confidential information.
3. This document is a component of the Oxford University Hospitals NHS Foundation Trust (OUH) Information Protection Policy and should be read in conjunction with the parent policy and its other components, and the Confidentiality and Disclosures component of the Information Governance Policy.

Definitions

Personal identifiable data (PID)

4. Information or data which can identify an individual, either on its own or when linked to other data to which the holder has access. Personal information is said to be *sensitive* if it includes details of the individual's health or physical condition, sexual life, ethnic origin, religious beliefs, political views, criminal convictions. For this type of information even more stringent measures must be followed to ensure that the data remains secure.

Safe haven

5. A secure, access-controlled location on OUH premises where person-identifiable information can be received, held, and communicated securely according to the procedures described herein.

Virtual safe haven

6. A designated rôle or named individual with responsibilities for receiving and communicating person-identifiable information securely according to the procedures described herein and providing a safe haven function that is virtual rather than physical. It will apply to a limited number of staff who require access to identifiable data to manage data quality and link records.

Primary and secondary use

7. The term *primary use* covers the use of information for direct patient care. *Secondary use* includes all other uses, including audit, service evaluation, research, commissioning, contract management and reporting. PID used for secondary purposes should be pseudonymised or anonymised to protect confidentiality.

Policy

8. All staff handling person-identifiable data must comply with the safe haven procedures below. Existing processes that are using patient identifiable information may need to be modified to be in line with this policy.

Safe haven procedures

When is a safe haven required?

9. A safe haven is required whenever personal information is being received, held or communicated, especially where the information is sensitive. There must be at least one area designated as a safe haven on each of OUH sites.

10. Internal flows of PID between departments and external flows to other NHS or non-NHS agencies must always be transmitted to a designated safe haven or virtual safe haven and must be consistent with the Confidentiality and Disclosures policy (a component of the Information Governance Policy).

OUH safe havenst

The following areas are currently used as safe havens:

- all locations occupied by the information team;
- all locations occupied by finance teams;
- all health records libraries;
- risk management (Manor House);
- legal services (Stable Block 1st floor);
- all locations occupied by Digital Services;
- pharmacies on all hospital sites;
- clinical secretarial and administrative offices.

Location/security arrangements

11. Safe havens should be located in areas that are secured by an ID badge-operated lock or a coded key pad with the code available only to authorized staff. Windows in ground floor areas must be lockable, and identifiable information kept out of sight. The area should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.

12. Paper records containing personal identifiable information must be stored in locked cabinets when not in use.

13. Computers and other digital devices must be password-protected, not left on view or accessible to unauthorized staff, have a secure screen locking function, and be switched off when not in use.

14. Staff working in safe havens must have appropriate training in confidentiality and safe record handling.

Authorization of safe havens

15. For an area to be designated as a safe haven a registration form (obtainable from Information Governance) must be completed and approved by the Information Governance and Data Quality Group. Safe haven areas will need to demonstrate compliance with security requirements above as well as adequate staff training.
16. The existing 'safe haven' areas listed above should aim to achieve registration by 31st December 2023.

Sharing information from safe havens

17. When information held within a safe haven needs to be shared this must be undertaken in accordance with the Confidentiality & Disclosure and Pseudonymisation & anonymisation policy components of the Information Governance Policy. Consult the Caldicott Guardian for advice when necessary.

Document History

Version	Date	Author(s)	Comment
2.2	August 2023	Dr Chris Bunch Data Protection Officer	Approved by TME 03/08/2023
2.2d	May 2023	Dr Chris Bunch Data Protection Officer	Routine updates
2.1	February 2018	Dr Chris Bunch Caldicott Guardian	Updated for Data Protection Act 2018
2.0	September 2016	Dr Chris Bunch Caldicott Guardian	Updated as a component policy document of the Information Protection Policy. Approved by IGDQG
1.1	March 2012		Adapted to new OUH Policy Format / IGG review
1.0	March 2011		Approved by OUH Trust Board

Pseudonymisation and anonymisation: policy and procedures

Introduction

1. NHS organisations are required to have policies and procedures to ensure the safe and confidential handling of personal information.
2. This document describes a framework for the safe handling of patient data for purposes other than direct care at Oxford University Hospitals NHS Foundation Trust (OUH).
3. This document is a component of the OUH Information Protection Policy and should be read in conjunction with the parent policy and its other components (notably the Safe Haven policy), and the Confidentiality and Disclosures component of the Information Governance Policy.

Definitions and general considerations

4. The terms **data** and **information** are commonly used interchangeably, and this document makes no distinction between them.
5. The term **patient (or person)-level data** refers to data relating to separate, individual patients or people. Data relating to a single individual may or may not be **linked** to other data sets relating to the same individual, usually be means of a unique identifier common to all such data sets. Linking data increases the chance that the individuals to whom it refers may be identified.

Personal data[1]

6. "Personal data" means any information relating to an identified or identifiable individual. "Identifiable individual" means an individual who can be identified, directly or indirectly, in particular by reference to:

   (a) an identifier such as a name, an identification number, location data or an online identifier; or

   (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

7. The use of personal data is subject to the requirements of the Data Protection Act (2018) and the UK General Data Protection Regulation. These apply only to living individuals, but the duty of confidentiality remains after death, and access to records of the deceased (as well as the living) is covered by the Access to Health Records Act 1990.

[1] As defined by the Data Protection Act 2018 (p. 3).

Confidential patient information

8. The NHS Act 2006 considers information about patients to be "confidential patient information" where—

    - the identity of the individual in question is ascertainable—
        - from that information, or
        - from that information and other information that is in the possession of, or is likely to come into the possession of, the person processing the information, and
        - that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual.

9. In addition to the statutory requirements of data protection and other relevant legislation[2], personal confidential data is subject to the common law duty of confidentiality. In brief, this normally requires the patient or service user's permission for any use other than the primary purpose for which it was obtained.

10. The term *patient identifiable information (PID)* is often used loosely to refer to personal data and/or patient confidential data. In the health and social care setting it is generally always safer to consider it to be confidential.

Primary and secondary uses of data

11. The term *primary use* covers the use of information for *direct patient care,* also known as *individual care.* Individual patients and service users need to be identified and therefore both personal data and confidential patient information are typically required to deliver care.

12. The scope of direct care includes both clinical and supporting administrative and assurance activities such as local clinical audit by the care team, clinical correspondence, appointments and scheduling.

13. *Secondary use* includes all other uses, including research, national clinical audits, commissioning, service planning, contract management, financial accounting and reporting.

14. Confidential patient data used for secondary purposes must normally be de-identified to maintain confidentiality. Exceptions to this rule are detailed below.

De-identification: anonymisation, aggregation, and pseudonymisation

15. The risk of identification of individuals from their data can be reduced by various means of de-identification or 'privacy-enhancing' technology. *Anonymisation* makes re-identification virtually impossible or at least very difficult. It involves the removal of all identifying characteristics, such as name, address, date of birth,

[2] For example, the Human Rights Act 2008, The Freedom of Information Act 2000, The NHS Act 2012 and associated legislation.

NHS/hospital record numbers etc. Even then, re-identification may be possible[3] if other sources of data regarding the individual are available, and especially if the data contains details of the patient's condition and/or the circumstances in which it was collected.

16. Anonymised data may be person-level, linked or not linked, or it may be *aggregated* so that the identity of individuals is completely removed. Anonymised data falls outside the scope of data protection legislation although linked anonymized data may not by virtue of the use of a unique identifier for linkage. Anonymised data also falls outside the scope of the National Data Opt-out.

17. *Pseudonymisation* is a process of de-identification in which the data fields that identify the individual may be retained but their contents are replaced with random or scrambled data. A unique identifier is typically included (so that data sets from the same individual can be linked) and a separate 'key' table created which pairs the unique identifier with an actual identifier such as the NHS Number. Provide the recipient of a pseudonymised data set does not have access to the key table, the data in their possession is effectively no different to linked anonymized data as described above.

18. The Data Protection Act and UK GDPR treat pseudonymised data as personal data and so it remains subject to the same restrictions as the personal data from which it originates. However, the de-identification process goes a long way towards protecting confidentiality.

19. In general, anonymised data is preferable to pseudonymised data for most secondary uses. Where it is considered essential to be able to refer back to the actual patient then pseudonymised data should be used. Such 'look-backs' are potential breaches of confidentiality and must always be justified and documented.

Disclosure of identifiable information for secondary purposes

20. There are occasions when personal confidential information may be disclosed for reasons other than direct care. Further information is available in the Confidentiality and Disclosures component of the Information Governance policy. In most instances, patient consent will be required in order to satisfy the common law duty of confidentiality, although this may be set aside in the following circumstances —

    - legal imperative: statutory requirement, court order;
    - overriding public interest; for example, to prevent death, serious injury or serious crime;
    - when consent is impracticable or impossible to obtain and there are good reasons to share the data e.g. for research, the Confidentiality Advisory

3 Ohm P (2010) Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Review 57; 1701.

Group of the Health Research Authority can recommend that the requirement for consent be set aside via Section 251 of the NHS Act.

Policy

21. All staff handling and/or person-identifiable data for secondary uses (non-direct patient care) must give due consideration to the descriptions above and ensure that an appropriate de-identification process is followed or, if it is essential to disclose identifiable data, then this is done lawfully, in line with the Caldicott Principles, and properly documented via a Data Protection Impact Assessment (DPIA), data sharing agreement or both.

Procedures for pseudonymisation

Business processes

All business processes that include personal data must be documented. Business processes can include but are not limited to:

- the process of using patient information for primary uses;
- the process for using patient information for secondary uses;
- the use of patient information for a combination of primary and secondary uses.

The business process for primary use includes, but it is not restricted to; appointment bookings, management of waiting lists or inputting test results. At this stage there is heightened importance on the accuracy and timeliness of the information. All information recorded about a patient should be recorded in line with the NHS Records Management Code of Practice 2021.

All business processes must be regularly reviewed to monitor the impact of de-identifying the data.

Pseudonymisation

Staff should only have access to the information that is necessary for the completion of the business activity with which they are involved, in keeping with the Caldicott Principles. When possible, pseudonymisation should be applied to patient identifiable data used for secondary or non-direct care purposes.

The aim of pseudonymisation is to obscure the identifiable data items within the records sufficiently to reduce the risk of identification of the data subject to acceptable levels.

Pseudonymised data should still be used within a secure environment (safe haven[4]) with access restricted to a need-to-know basis.

[4] See the accompanying Safe Haven component policy.

Pseudonymisation can be achieved by replacing patient identifiers with a pseudonym or the use of the value ranges: for example, age instead of date of birth. When pseudonymisation techniques are consistently applied, the same pseudonym is provided for individual patients across different data sets and over time. This allows the linking of data sets and other information which is not available if the patient identifiable data is removed completely or a different pseudonym is used for each data set.

Thus, to effectively pseudonymise data:

- each data field that identifies or may identify the data subject must have a unique pseudonym;
- pseudonyms must be used in place of NHS Numbers and all pseudonymised fields should be of the same length and formatting to ensure readability. For example, to replace NHS Numbers in existing report formats the output pseudonym should generally be of the same field length, but not of the same characters, e.g. 5lL7 TWX 619Z. Letters should be used within the pseudonym for an NHS Number to avoid confusion with original NHS numbers;
- pseudonymisation must only be performed on copies of the original data to ensure its preservation and integrity;
- different pseudonym values must be generated for each separate use of the same dataset, whether for internal use or external transmission;
- data prepared for secondary use must only contain the data items that are required, pseudonymised as appropriate (Caldicott Principle 5);
- pseudonymised data must be kept as securely as identifiable data.

Document History

Version	Date	Author(s)	Comment
2.2	August 2023	Dr Chris Bunch Data Protection Officer	Approved by TME 03/08/2023
2.2d	June 2023	Dr Chris Bunch Data Protection Officer	Minor updates
2.1d	July 2020	Dr Chris Bunch Data Protection Officer	Policies and procedures combined.
2.0	October 2019	Dr Chris Bunch Caldicott Guardian	Updated as a component of the Information Protection Policy (Separate Safe Haven policy)

Safe Haven and Pseudonymisation Policy 1.1	March 2012		Adapted to new OUH Policy Format / IGG review
Safe Haven and Pseudonymisation Policy 1.0	March 2011		Approved by OUH Trust Board

Clear screen and desk policy

Introduction

1. The purpose of this policy is to ensure that confidential information on paper or online is held securely and kept away from prying eyes. Keeping information safe will help to reduce the risk of breaches of confidentiality, theft, or fraud due to confidential information being left unattended and visible.
2. This document is a component of the Oxford University Hospitals NHS Foundation Trust (OUH) Information Protection Policy and should be read in conjunction with the parent policy and its other components.

Scope

3. This policy applies to any place where confidential information may be seen by unauthorised persons: for example, on a screen or printed material left out on desks whether on premises or at home.
4. All staff and contractors employed by OUH must abide by this policy.

Policy

5. Staff (including contractors) working with confidential information must at all times ensure that:
    1. when unattended, their workspace is cleared of any documents or other items containing confidential information, and that any screens are either turned off or password-protected;
    2. confidential information is only printed if absolutely necessary;
    3. before printing their default or chosen printer is correct;
    4. when printing to a shared printer the printer is locked: if this is not possible, the printed material must be collected from the printer without delay;
    5. paper documents containing confidential information are shredded or placed securely in confidential waste bins when no longer required;
    6. all portable computing & storage devices such as USB data sticks, dictaphones, mobile phones, tablets and laptops are placed out of sight and preferably locked away when not actively being used;
    7. desks and other workspaces are left sufficiently clear at the end of each working day to permit cleaning staff to perform their duties safely;
    8. Smartcards are removed from card readers when users are away from their desks; tap-and-go users must tap out at the end of each session;
    9. desktop computers and laptops are not left logged on when unattended: screens must be locked, or the device closed;

10. if sensitive or confidential information is visible to an unauthorised person standing close to it, the person is asked to move away to protect the confidentiality of the information.

Monitoring compliance

6. The Information Governance team will monitor compliance with this policy and report outcomes to the Digital Oversight Committee.

Document History

Version	Date	Author(s)	Comment
1.2	August 2023	Dr Chris Bunch, Data Protection Office	Approved by TME 03/08/2023
1.2d	June 2023	Dr Chris Bunch, Data Protection Office	Minor updates
1.1d	May 2020	Dr Chris Bunch, Data Protection Officer	Routine update
1.0	July 2020	Nuala Buchan-Brodie	Created as a component of the Information Protection Policy

Patient Photography and Video Policy

Introduction

1. Making photographic and video recordings of patients is a common clinical practice. Recordings may be made for the purpose of providing a clinical record, for teaching, diagnosis, treatment planning, quality assurance, clinical governance, publication, research and as legal evidence.
2. All recordings made within the Oxford University Hospitals NHS Foundation Trust (OUH) are subject to legislation which provides the patient with rights of confidentiality, and protection against the unlawful processing of data.
3. The policy and accompanying guidelines set out the acceptable procedures for OUH. They are not intended to be over-restrictive but aim to ensure all parties are protected and aware of their responsibilities.
4. In this document the term 'recording' is used to refer to a patient photographic or video recording made on any device.
5. This document is a component of the Information Protection Policy and should be read in conjunction with the parent policy and its other components.

Scope

6. This policy applies to all recordings of patients in all formats, with the following exceptions:
   - radiological images (including MRI, CT, ultrasound);
   - macro/micro images of pathological specimens;
   - ophthalmic images, endoscopy, proctoscopy, colposcopy, etc.;
   - close-up images of the operative field during surgery.
7. All OUH employees, staff with honorary contracts, contractors or guests who make recordings of patients in the course of their work are required to follow this policy and the companion guidelines.
8. All recordings are subject to this policy irrespective of who owns the equipment or the materials on which they are produced.

Professional requirements

9. Medical staff are bound by the General Medical Council's guidance *Making and Using Visual and Audio Recordings of Patients*.
10. Clinical Photographers are bound by the Institute of Medical Illustrators' guidance: *The Code of Professional Conduct (2023)*.

Policy

11. All recordings will be regarded as part of the patient's confidential medical record. Consequently, such recordings are entitled to the same degree of protection and should be treated with the same respect and confidentiality as all other components of the patient's medical record. There must be a fully justifiable purpose for any photographic or video recordings to be made.
12. Where the recording is for direct patient care, written consent or a signed consent statement is not required although, as with other investigations, it is best practice to explain the purpose of a recording, and that it will be stored as part of their secure confidential treatment record.
13. Formal, written consent is required for recordings which will or may be used for purposes other than direct clinical care, for example for teaching, research or publication, whether the patient is the main subject of the recording or incidental to it.
14. Patients may withdraw consent at any time.
15. All recordings should be stored securely in the patient's digital medical record and be available for disclosure at the request of the patient or their representative.
16. Copyright in all recordings made by staff in the course of their work belongs to OUH and must not be transferred.

Responsibilities

17. Oxford Medical Illustration is responsible for:
    - developing, reviewing and maintaining this policy and associated guidelines;
    - providing expert advice and guidance;
    - setting an example of good practice for all staff.
18. *Chief Officers, Divisional Directors, Divisional Directors of Operations, Nursing Directors and Clinical Directors* are responsible for ensuring the distribution, communication, implementation of and compliance with the policy and guidelines the policy throughout OUH and their Division.
19. *Heads of Service, Clinical Leads, Consultant and Senior Nurses* are responsible for informing all new and existing staff, contractors and other persons making recordings about this policy and ensuring that they comply with its requirements.
20. *Individual OUH staff* must familiarise themselves with the policy and guidelines before making recordings and comply with its requirements.

References

The common law duty of confidentiality
The Access to Health Records Act (1990)
The Children Act (1989 and 2004)
The Copyright, Designs and Patents Act (1988)
The Data Protection Act (2018) and the UK General Data Protection Regulation
Mental Health Act 2007
Mental Capacity Act 2005
Obscene Publications Act 1964
Copyright & Patents Act 1988
Professions Supplementary to Medicine Act 1960
Human Rights Act 1998
Freedom of Information Act 2000

Document history

Version	Date	Author(s)	Comment
2.6	August 2023	Dr Chris Bunch Data Protection Officer	Approved by TME 03/08/2023
2.6d	May 2023	Dr Chris Bunch Data Protection Officer Roddy McColl and Emily Arthur Oxford Medical Illustration	Minor updates
2.5d	May 2022	Dr Paul Altmann, CCIO Roddy McColl & Warwick Baggaley	Minor routine updates
2.4	March 2021	Dr Paul Altmann, CCIO Roddy McColl & Warwick Baggaley	Updated for EPR & PowerChart Touch and clarifications of consent for direct care
2.3	November 2018	Dr Chris Bunch Caldicott Guardian Roddy McColl & Warwick Baggaley	Added reference to linked guidelines
2.2	February 2018	Dr Chris Bunch Caldicott Guardian Roddy McColl & Warwick Baggaley	Updated for the Data Protection Act 2018
2.1	January 2016	Dr Chris Bunch Caldicott Guardian Roddy McColl & Warwick Baggaley	Adapted as component of the Information Protection Policy
2.0	December 2016	Roddy McColl & Warwick Baggaley Oxford Medical Illustration	

Registration Authority Policy and Procedures

Introduction

1. The Registration Authority (RA) is the function responsible for the identity checks of prospective smartcard users and assigning an appropriate access profile to the health professional's role as approved by Oxford University Hospitals NHS Foundation Trust (OUH). The roles and responsibilities of the RA are defined by NHS policy, the key components of which are included here for emphasis and ease of access.
2. NHS England smartcards are similar to chip and PIN bank cards and enable healthcare professionals to access clinical and personal information appropriate to their role. A smartcard used in conjunction with a passcode, known only to the smartcard holder, gives secure and auditable access to national and local Spine-enabled health record systems.
3. This document is a component of the OUH Information Protection Policy and should be read in conjunction with the parent policy and its other components.

Policy

4. The smartcard registration process is operated locally by the OUH Registration Authority (RA) Office. It is required by and must conform to National Registration Authority Policy. The department will ensure ensuring tight control over the issue and maintenance of smartcards, whilst providing an efficient and responsive service that meets the needs of the users.
5. This policy applies to the Registration Authority Office[1], its staff, and to all personnel using a smartcard at OUH.

Responsibilities

6. The Registration Authority Manager has overall responsibility for RA governance and processes, the RA Offices, and RA Agents. This responsibility cannot be delegated.
7. The Director of Workforce has overall responsibility for ensuring that the Resources Department at OUH is able to support the RA function by:
    - ensuring all users are recorded on ESR (Electronic Staff Record);
    - ensuring all ID documents are in ESR and visible on TRAC;
    - sending the Starters and Leavers forms to the RA/Smartcard Office so that access to systems can be added or revoked;
    - notifying the Smartcard Office of extended honorary contracts.

[1] Also known as the Smartcard Office, currently situated in the Academic Street, Level 3, The John Radcliffe Hospital

8. RA Agents are responsible for day to-day implementation of the registration procedures below.
9. Smartcard holders are responsible for keeping their cards safe and secure and ensure that they are not used by anyone else.

Registration procedures

ESR/RA link

10. The management of smartcards and users will be carried out through the Electronic Staff Register (ESR)/RA interface for all staff on ESR. All other smartcard holders will be managed manually on the NHS Care Identity Service (CIS) system (which is gradually being replaced by Care Identity Management).
11. Role based access control (RBAC) will be maintained by the RA Manager and approved through the Digital Oversight Committee (DOC) on a regular basis. If required, RBAC definitions may be amended at any time for operational purposes without the reference to DOC, but any changes will be notified to DOC as soon as possible afterwards;
12. The same RBAC list will be used to allocate roles to temporary (non-ESR) staff if justifiable and requested by their line manager. Registrations using this route will require an RA02 form or the current version of the electronic request form to be completed by the requesting manager and sent by internal email to smartcards@ouh.nhs.uk.

New starters

13. The HR department will notify the RA Office of all new staff and their start date.
14. The RA Office will register all staff who are required to use the Cerner Millennium electronic patient record (EPR) as a matter of course, whether they will need a smartcard or not.
15. In order to register, new staff members must bring suitable forms of identification[2] to the RA Office.
16. The RA office will create network and email accounts for new starters so that they are available on their induction day.
17. An RA01 form will be completed, and the user will be processed either as a new registrant or, if they already hold an NHS smartcard, add the necessary RBAC profile/s to the smartcard.
18. All users will be associated in ESR/CIS and photographs uploaded into the active directory folder.
19. The RA Office will set up new clinical staff to use the virtual workstations.

[2] Currently two forms of photo ID and one form of ID with name and address. More details can be obtained from the Office (01865 5) 72719.

20. The RA Office will set up new clinical staff to use SEND, which is used to record patients' vital signs. There are a few exceptions that will not be added to SEND i.e. staff working in maternity or paediatrics.

21. All staff when issued with a smartcard must sign to acknowledge that they have read and understood the policies and procedures governing the use of smartcards[3]. This is automated when the user inserts their smartcard into the keyboard of the computer for the first time.

22. All medical staff registered with the GMC will have a PACS (picture archiving and communication system) account created for them and will be required to complete Insight Web Training before using the system. They will also be required to complete the appropriate EPR Training. The RA Office will create their accounts on My Learning Hub and send details onto them.

Leavers

23. The HR and Payroll departments send signed documents from managers regarding leavers. These are processed on a daily basis. The RA Office will ensure that employment end dates are applied EPR roles and network accounts.

24. The RA Office will deactivate or update leavers' role profiles in CIS as soon as practicable after they leave or before and will notify Digital Services to deactivate their network/email/SEND accounts.

25. Staff permanently leaving the NHS must hand their smartcard back to their line manager or to the RA Office so that their roles may be revoked and the smartcards destroyed. Staff leaving to work in another NHS trust may continue with the same smartcard, but the roles within the OUH Care Identity Service will be revoked.

Revocation of smartcards

26. There are occasions when it is necessary to deactivate a smartcard by revoking the smartcard certificate. Reasons for this include:

    - the smartcard is lost or stolen;
    - there has been some other security breach associated with the smartcard or smartcard certificate;
    - the user is no longer employed by an NHS organisation.

27. Revocation tasks can only be carried out by RA team members. Revocation renders the smartcard useless.

Lost/stolen or damaged smartcards:

28. Lost or stolen smartcards must be reported to the RA Team as soon as it is practicable by either emailing smartcards@ouh.nhs.uk or calling 01865 572719. The card will be destroyed, and the user will need to complete an incident form via Ulysses before a new card can be issued.

[3] See also the Acceptable Use policy component of the Information Protection policy.

29. Damaged smartcards must be reported to the RA Office. and will be replaced or repaired.

Smartcard passwords

30. Users will be required to enter a smartcard password when collecting their cards.
31. Users who have forgotten their passwords or suspect that it may be known by another or have been locked out due to three failed login attempts; should either visit the RA Office or find a card un-locker within their area of work.
32. Staff can register for the Self-Service Unlock Process.

Locums, agency and bank personnel:

33. The following points should be considered:
    - Staff working as part of a team may not require a smartcard to fulfil their role;
    - Some staff may already have been registered and will only require a role profile added;
    - Those already having a smartcard may not have sufficient training in its use in their new role. This will need to be organised by their departmental manager.
34. All temporary staff requiring access to the electronic patient record system (EPR) will be registered for a smartcard once the following processes have been completed:
    - an RA02 form is completed by their line manger within the department they will be working in. This will be submitted electronically and secured with the temporary worker database;
    - the required ID documentation has been seen;
    - access will initially be granted for one month only in which EPR training will need to be completed. Once training has been completed, access will be given for 3 months at any given time. For further extensions, a RA02 form will need to be completed by the line manager;
    - should the temporary staff member change department, a new RA02 form will need to be completed by their new line manager;
    - it is the responsibility of the line manager to notify the Smartcard Office when the user leaves the Trust so as access can be revoked as soon as possible.
35. This staff group includes:
    - locums;
    - NHS Professionals staff;
    - clerical agency staff;
    - agency staff for AHP and other groups

Training for staff

Medical staff and students

36. All medical staff joining the Trust will need to complete EPR training before their smartcards are activated, and will be set up on the e-Learning system (My Learning Hub) and emailed regarding the required training.
37. This process also applies to medical students before receiving an active smartcard.

All other staff:

38. It is line managers' responsibility to organise EPR Training for their staff.

Short term access (Tenens) cards:

39. Clinical departments have been issued with short-term access smart cards known as *Tenens cards.* These cards are only for locum/agency staff that are required to fill a post at short notice.
40. The Tenens system is maintained by Digital Services and is closely monitored by the RA manager. Regular audits are completed and departments notified via email of any required actions.
41. Lost or stolen smartcards not returned will only be replaced once an incident form has been completed.

Local Support

42. Application users who need support should contact the IM&T Service Desk on 01865 222822. The RA Team have access to the helpdesk system and will be able to access the call information.

Smartcard terms and conditions

43. Misuse of smartcards, intentional violation of confidentiality or disclosure of passwords constitutes a serious breach of this agreement and of Trust policy, and may result in disciplinary action.
44. Smartcards must not be defaced or damaged for example by placing stickers on top of photographs. A breach of security could result if the user cannot be identified during the unlocking process, for example.

Audit

45. The management and use of Smartcards will be subject to internal and external audit to ensure that national and local policy is being followed. Specifically, auditors will look to confirm that:
    - smartcards are handled securely by users;

- unused Smartcards are stored safely;
- RBAC role allocation and de-allocation is performed appropriately.

Document history

Version	Date	Author(s)	Comment
2.8	August 2023	Dr Chris Bunch Data Protection Officer	Approved by TME 03/08/2023
2.8d	May 2023	Helen Juggins Chris Bunch	Minor updates
2.7d	May 2022	Helen Juggins Chris Bunch	Routine policy update
2.6	July 2019	Helen Juggins Chris Bunch	Added SEND to new starters (para. 16)
2.5	February 2018	Helen Juggins Chris Bunch	General policy update for GDPR
2.4	January 2017	Helen Juggins	Updated and created as a component policy document of the Information Protection Policy

Information Security Policy for Third-party Suppliers

Introduction

1. Oxford University Hospitals NHS Foundation Trust (OUH) requires contracts and agreements with third-party (external) service providers and suppliers. Many of these contracts and agreements will involve the use and storage of identifiable and sensitive information. There is a legal obligation to ensure that such contracts and agreements contain clauses to ensure appropriate technical and security measures are in place to protect information.
2. This document is a component of the OUH Information Protection Policy and should be read in conjunction with that Policy and other component policies. is accompanied by a procedure which outlines the process that must be followed before any contracts and/or agreements are made with a third-party supplier.
3. Compliance with these policies will ensure that OUH is compliant with its legal responsibilities, reduce the risk of an information security breach, and provide assurance to our staff and patients that their information is being properly managed.

Scope

4. This policy applies to all employees, volunteers or other individuals working on behalf of OUH who are responsible for entering into any agreement or contract with third-party suppliers that involves the third-party having access to or receiving personal data relating to patients or staff, or sensitive information relating to corporate affairs which, if disclosed, could have a detrimental effect on the running of the organisation.
5. The policy covers both digital and paper-based information and applies where information is shared with a third-party supplier, their employees or any party within their supply chain, and where the third-party may have access to OUH's digital systems or to paper-based information held on or off-site. It also applies when individuals have indirect access to information i.e. staff/cleaners accessing rooms that may contain patient Information, individuals transporting patient information etc.

Aims and objectives

6. The primary aim is to ensure that personal data is kept safe and secure and that OUH complies with its statutory duties in the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) or any successor legislation, the Human Rights Act 1998, and the common law duty of confidentiality.
7. It will ensure that all third-party suppliers who enter into an agreement or contract with OUH are clear about their obligations to information security and confidentiality, and have the relevant technical and security measures in place to meet data protection legislation and privacy requirements.

Definitions

8. **Third-party supplier** – an individual, company or organisation that supplies goods or services to OUH including any subsidiary of OUH.
9. **Personal data** – information/data relating to an identifiable person.
10. **Special category data** – information/data covered by UK GDPR Article 9.
11. **Sensitive corporate information** — confidential information which, if disclosed, could have a detrimental effect on the organisation.
12. **Data processor** - means a natural or legal person, public authority, agency or other body which processes personal information on behalf of OUH.

Responsibilities

13. In addition to responsibilities listed in the parent Information Protection Policy:
14. The Procurement Lead is responsible for following the process as set out in the accompanying Third-party Information Security Procedure and ensuring that contracts are completed and managed in accordance with this process.
15. The Information Governance Team is responsible for the dissemination of this Policy and its associated Procedure across the Trust. The team is responsible for providing appropriate support and advice to IAOs, service leads, managers and staff to ensure that this Policy is understood and adhered to. As required, the team will review Third-party Supplier Questionnaires to ensure that appropriate security standards have been met. The team will provide advice to the Procurement department and those entering into contracts and agreements about the completion of details of processing in the information protection protocol or similar annexes and the addition of further contract terms.
16. The Cyber Security Analyst will review completed Third-party Supplier Security Questionnaires, undertake risk assessments and identify where risks require mitigation and advise on any additional contract terms as appropriate.
17. Service leads/Managers must ensure that they and their staff comply with this policy and procedure when entering into any new contracts or agreements with third-party suppliers, monitor compliance, and report any non-compliance to the Information Governance Team.
18. All staff responsible for buying goods and services must read, understand and comply with this Policy and seek clarification from their service leads or managers if necessary. Staff intending to enter into agreements involving the use of personal data are required to complete a Data Protection Impact Assessment (DPIA) to demonstrate that they have considered the legal basis for using personal data and how it will be managed securely. Further information about completing a DPIA can be found in the Trust Information Governance Policy.

Policy

Contract/agreement evaluation

19. Any contract or agreement involving the processing of identifiable information or sensitive corporate information must describe how information will be managed securely
20. Evaluation will entail screening prospective purchases for the use of identifiable or sensitive information. Contracts and agreements falling into this category will require investigation. Third-party suppliers will be sent a Supplier Security Questionnaire to complete which requests evidence about company information security arrangements.
21. Completed questionnaires will be reviewed by the Cyber Security/Information Governance teams. No contracts or agreements will be progressed that do not demonstrate sufficient supplier security arrangements.

Contract/agreement arrangements

22. A contract/agreement should exist between OUH and third-party supplier to protect both parties. Contracts using NHS Standard Contract Terms together with a completed Information Protection Protocol will contain the correct contract terms. Contracts/agreements falling outside of these will need to be checked to ensure that they contain the correct terms. In some cases it will be necessary for additional contract clauses to be added to a Schedule of the contract. Examples include, but are not limited to, additional security terms and details of the information being processed. A proforma to effectively capture this information can be found in the accompanying Information Security Procedure for Third-party Suppliers.
23. Completed contract documentation will be uploaded to the contract entry within the OUH contract register.

Document History

Version	Date	Author(s)	Comment
1.0	Aug 2023	Dr Chris Bunch Data Protection Officer	Approved by TME 03/08/2023
1.0d	May 2023	Dr Chris Bunch Data Protection Officer	Updated as component of the Information Protection Policy
0.6	Nov 2020	Nuala Buchan Brodie IG Manager Gary Welch Director of Procurement Chis Caley CyberSecurity Analyst	Not widely released