Information Protection Policy

Category:	Policy
Summary:	Main policy document for information protection
Equality analysis undertaken:	February 2015.
Valid from:	1st August 2020
Date of next review:	July 2023
Approval Date/ via:	29th July, 2020/DPO
Distribution:	Trust-wide
Related documents:	Acceptable use policy Network security policy Mobile devices policy Safe haven policy Pseudonymisation and Anonymisation: Policy and Procedures Clear desk and screen policy Photography and video policy & guidelines Registration Authority policy
Author:	Dr C Bunch, Caldicott Guardian and Data Protection Officer
Further information:	Information Governance
This document replaces:	Information Protection Policy v5.5

Lead Director: Chief Digital and Partnership Officer

Issue Date: 29th July, 2020

Contents

Introduction

1. NHS organisations are required by law to have written policies and procedures covering the collection, storage, processing and disclosure of personal and confidential information in both manual and electronic systems.
2. The Oxford University Hospitals NHS Trust is committed to ensuring that all sensitive, identifiable and business information is held legally and securely.
3. The principal information types to which this policy applies are patient identifiable information within healthcare records, staff information, corporate information (financial and business), and intellectual property.

Policy statement

4. All employees and parties processing personal data for and on behalf of the Trust must adhere to this policy and must seek to prevent improper or unlawful disclosure of information collected, processed and stored by the Trust (including patient, business, administrative, research, professional and staff information).
5. The Oxford University Hospitals NHS Foundation Trust is the Data Controller for all personal information processed as part of its function.
6. The policy comprises this document and the following component policy documents:

Acceptable use policy: the responsibilities of users with respect to IM&T including internet use, email and social media
Network security policy: how the Trust's network and IT infrastructure will be secured
Mobile devices policy: governing the use of portable 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

7. Additional documents may be added as required and following approval by the Information Governance and Data Quality Group.

Scope

8. This policy applies to all areas of the Trust, and all employees of the Trust, including individuals employed by a third party, by external contractors, as voluntary workers, as students, as locums or as agency staff.

Aim

9. The purpose of this Policy is to ensure compliance with the requirements of the Data Protection Act 2018, the General Data Protection Regulation (GDPR) 2016, the Security of Network & Information Systems Regulations (NIS Regulations) 2018, and other relevant legislation.

Definitions

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

- *Data and information* — these terms are used interchangeably;
- *Senior Information Risk Owner (SIRO)* – the SIRO is an executive member of the Trust Board who has delegated responsibility for ensuring that information risk is properly identified and managed and that appropriate assurance mechanisms exist;
- *Caldicott Guardian* — a senior individual who oversees and advises on the confidentiality and of handling personal identifiable information;
- *Data Protection Officer* — a senior individual having expert knowledge of data protection matters and detailed understanding of the Trust's business and the purposes for which it processes data, and who advises the Trust (as data controller) on all aspects of its responsibilities for data and information protection and compliance;
- *Information Asset* – an electronic or paper-based system, (e.g. database/spreadsheet) used to process personal identifiable data, record volumes of personal identifiable data on a regular basis or set time frame.
- *Information Asset Owner (IAO)* – the individual responsible for the overall management of the processing of personal data in an information asset. The IAO is directly accountable to the SIRO (or delegated deputy) in this role and must provide assurance that information risk is managed effectively for the information assets they own;
- *Information Asset Administrator/Manager (IAA/IAM)* – the day to day system manager of an information asset, usually responsible for backups and user management;
- *Information Asset Register (IAR)* – the Trust's online system used to register information assets, on which the ownership, management, processing, storage, risk, access, retention, transfers of data, business continuity, recovery of the data on that system are defined;
- *Personal Identifiable Data (PID)* – data which can identify an individual or individuals either on its own or if combined with other data which is in the possession of, or is likely to come into the possession of, the holder of the data.
- *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) organization, 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* – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- *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.

Responsibilities

11. The *Chief Executive* as the Accountable Officer has responsibility for ensuring that the Trust complies with its statutory obligations and Department of Health and Social Services Directives.
12. 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.
13. The *Caldicott Guardian* is responsible for overseeing and advising on processes to satisfy the highest standards for handling personal identifiable information.
14. The *Data Protection Officer* advises the Trust, as data controller, on all aspects of its responsibilities for data and information protection and compliance, supports the Trust to ensure that it has a legal basis for its data processing, advises on relevant procedures and procedures, and monitors compliance with data protection regulations and relevant organisational policies.
15. The *Information Governance and Records Manager* is responsible for supporting and monitoring the implementation of this policy.
16. *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.
17. 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.

Training

18. Training required to fulfil this policy will be provided in accordance with the Trust's training needs analysis. Management and monitoring of training will comply with the Trust's *Learning and Development Policy*. This information can be accessed via the learning and development pages on the Trust intranet.

Monitoring compliance

19. Compliance with the document will be monitored in the following ways.

Aspect of compliance or effectiveness being monitored	Monitoring method	Responsibility for monitoring (job title)	Frequency of monitoring	Group or Committee that will review the findings and monitor completion of any resulting action plan
Policy implementation and staff compliance	Monitoring and investigation of information and IT-related incidents	Information Governance Manager. Divisional General Managers.	Following a reported incident	Information Governance and Data Quality Group
Policy implementation and staff compliance	Spot checks of departmental areas and audits	Information Governance Officer	Annually	Information Governance and Data Quality Group
Network security	Penetration testing, random checks and audits	Head of IM&T Service Delivery	At least annually	Information Governance and Data Quality Group

Review

20. This policy will be reviewed in 3 years, as set out in the Policy for the Development and Implementation of Procedural Documents.

21. Component policy documents, as listed in paragraph 5, will remain under continual review and will be updated as required in response to changing circumstances, legislation or security threats. A summary of updates will be reported to the Information Governance and Data Quality Group at least annually.

Equality analysis

22. As part of its development, this policy and its impact on equality, diversity and human rights has been reviewed and an equality analysis undertaken (see appendix). As this policy applies to all staff equally, no detriment was identified to any group and no adjustments are required.

Relevant legislation

Data Protection Act 2018
General Data Protection Regulation 2016
Security of Network & Information Systems Regulations (NIS Regulations) 2018

Document History

Date of revision	Version number	Reason for review or update
April 2000	3.1	IG Toolkit requirement
May 2008	4.0	Routine update
June 2010	4.1	Minor update
March 2012	4.2	Minor amendments. Updated to new Trust policy format
February 2015	5.0	Extensively updated to incorporate IM&T security policies
November 2015	5.1	Updated to include confidentiality policy
November 2016	5.2	Updated to include safe haven policy
February 2018	5.3	Updated for Data Protection Act 2018
November 2018	5.4	Incorporates Patient Photography and Video Guidelines
July 2020	5.5	Minor updates and corrections and to include pseudonymisation and clear desk policies

Appendix 1: Equality assessment

Equality assessment: Information Protection Policy
February 2018 (reviewed)
Review date: *January 2021*
Lead person for policy and equality analysis *Information Governance Manager*
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 protect the information that the Trust holds and the confidentiality of personal information.*
Involvement of stakeholders *The policy has been developed by the Caldicott Guardian, Information Governance Team, IM&T Services and the Information Governance and Data Quality Group. It takes into account feedback from incidents, complaints, advice from 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.) *n/a*
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.*
How does the policy advance equality of opportunity? *n/a*
How does the policy promote good relations between groups? *n/a*

Network Security Policy

Introduction

1. The Trust 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 Trust'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 Trust systems is maintained. This policy document sets out the actions and responsibilities required to achieve these aims.
2. The Trust will ensure that the network is available when needed, can be accessed only by legitimate users, will contain complete and accurate information, and be able to withstand or recover from threats to its availability, integrity and the confidentiality of information therein. 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 non- technical measures;
    - undertaking regular security risk-assessments to ISO27001 standards, covering all aspects of the network that support the Trust'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.
3. This document is a component of the Trust's Information Protection Policy and should be read in conjunction with the parent policy and its components.

Scope

4. For the purposes of this policy, the network comprises the totality of the Trust'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 Trust or personally-owned if they are used for Trust business and/or communicate with the Trust's network. (See also the Mobile Devices policy.)
6. This policy applies to all electronic data systems used for the Trust's clinical and non-clinical activities, whether or not directly managed by the Trust's IM&T Services.
7. It applies also to the provision of access to the internet and the NHS N3 network (and any future replacement), "cloud computing services", and to all forms of remote access to the Trust's network and systems.

Responsibilities

8. The overall responsibility for information security rests with the Trust's Senior Information Risk Officer; day-to-day responsibility for the security of the physical IT

infrastructure is delegated to the Information Security Manager (presently a rôle of the Head of IM&T Service Delivery), through the Director of IM&T Services.

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 Trust's Information Governance Framework. The Trust' 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 Trust's Information Governance Framework.
11. Systems that are part of the network as defined above but which are not owned or directly managed by IM&T Services are the responsibility of the relevant Divisional Directors who must ensure compliance with this and other relevant Trust policies as they apply to those systems. Such systems include, *inter alia,* laboratory and radiology information systems.
12. Maintenance of this policy is the responsibility of the Information Security Manager.

User responsibilities

13. The responsibilities of users of the Trust'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

14. Network equipment will be housed in a controlled and secure environment. 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).
15. Smoking is forbidden on all Trust premises. Food and drink must not be taken into areas housing critical or sensitive network equipment.

Access to equipment

16. Physical access to network equipment must be strictly controlled and monitored at all times.
17. Where possible equipment room access should be controlled using the Trust's 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 Information Security Manager. In the event a key code is thought to have been compromised it must be changed immediately.
18. Entry to secure areas housing critical or sensitive network equipment is restricted to those who require access to carry out their jobs. The IM&T department 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.

19. Visitors to secure network areas must be authorised by the IM&T Services Information Security Manager or the Head of IM&T Service Delivery, 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.
20. 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 IM&TS staff with the required training. Visitors are not allowed into these areas unaccompanied.
21. The Trust has an agreement with Oxford Health Foundation Trust (OHFT) which allows OHFT designated space in the OCDEM Data Centre for its sole use. Designated OH 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 network and Trust systems

22. Trust 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 IM&T Services, who will report any breaches or suspicious activity via the Trust's incident reporting system (Datix).
23. All users must comply with the Acceptable Use Policy.
24. Access to the network for staff on Trust 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.
25. 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.
26. Users must always log out of Trust 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.
27. The Human Resources department will notify all leavers to IM&T Services, who will terminate their access.

Smartcards

28. Trust 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 .

29. 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 Datix.

Virtual workspace/desktop

30. The Trust uses virtual workspace/desktop services 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 the session from any convenient networked computer.

Tap-and-go

31. 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.

32. 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)

33. The Trust provides two wireless networks: OxNET-WLAN is the Trust's secure corporate wireless network. Access is only available to staff members authorised by IM&T Services and requires login using the standard Trust (Active Directory) username and password. The wireless network is logically co-terminus with the Trust's corporate wired network and gives access to all networked services including the NHS N3 network and the internet.

34. 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

IM&T services. It is possible to access OUH and NHS Mail email accounts, both directly and via a web browser, via this network.

35. All network logins will be logged. IM&T Services will undertake periodic access audits, and will investigate and report any inappropriate or suspicious events.

Connection of devices to the network

36. No device (PC, switch, hub, etc.) may be connected to the physical network (wired/wireless) without prior permission from IM&T Services. Only Trust-owned equipment is permitted to connect to the corporate networks, except in exceptional circumstances and with the approval of IM&T services. (See also the Mobile Devices and Acceptable Use Policies.)
37. 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 the requirements of the user's job and at the discretion of IM&T Services.
38. Users are not permitted to extend the network to other users by creating WiFi 'hotspots'.

Remote and third-party access

Virtual private network (VPN)

39. The Trust makes available secure VPN access to the Trust's network. Access may be granted according the requirements of the user's job and at the discretion of IM&T Services. The security of VPN access is primarily the responsibility of IM&T Services. Users should only access the VPN service from Trust devices or devices they own and have control over, and never from public computers.

Third party access

40. Third party access to the network may be granted for legitimate purposes such as system maintenance at the discretion of IM&T Services and (where access to patient identifiable data is possible) the Trust's 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

41. IM&T Services will ensure that all connections to external networks and systems have been documented on the Trust Information Asset Register. IM&T 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.
42. The Information Security Manager must approve all connections to external networks and systems before they commence operation.

Business continuity

43. IM&T 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 by the Information Security Manager on a regular basis.
44. The Information Security Manager 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.
45. 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.
46. 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).
47. Users are responsible for ensuring that their own data is backed up by storing their data on a network server.

Equipment procurement, deployment, maintenance and disposal

48. All network equipment and equipment connected to the network must be approved by IM&T Services and must meet agreed security standards.
49. 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

50. The Information Security Manager is responsible for ensuring that maintenance contracts are maintained and periodically reviewed for all equipment.

Equipment re-use

51. Where possible equipment will be reallocated if it is fit for purpose and supportable, otherwise IM&T Services will recommend that equipment reaching end-of-life be replaced.
52. 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. IM&TS 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.

53. The secure disposal of equipment not procured through IM&T Services is the responsibility of the Information Asset Owner Any storage media should pass through the IM&TS media destruction process described in para. 52 above.

Security monitoring and incident reporting

54. IM&T Services will ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.
55. The Information Security Manager is responsible for ensuring that a log of all faults on the network is maintained and reviewed.
56. IM&T Services will record any incidents in the IM&T Services call management system. In addition, all potential security breaches will be reported via the Trust's incident reporting system (Datix) and investigated. Serious incidents and weaknesses must be reported in accordance with prevailing NHS requirements.
57. Incidents involving systems not managed by IM&T Services must be reported by the relevant Information Asset Owner.

Document History

Version	Date	Author(s)	Comment
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

Acceptable Use Policy

Introduction

1. The Trust 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 the Trust'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 Trust's 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 Trust IT 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 Trust and system-specific policies and procedures for the operation and/or use of the resources;
    - Use or access only that equipment, services programs, information or data, for which they have specific authorisation;
    - Make reasonable efforts to protect passwords and to secure resources against unauthorized use or access;
    - Use only those usernames and passwords that have been issued to them personally for logging into Trust systems;
    - Respect the privacy and personal rights of data subjects (e.g. patients) and other users;
    - Respect the good name and reputation of The Trust in all electronic communications with those within and outside the Trust.

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, an 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 (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), and the Oxfordshire Care Summary (OCS), 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.
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. Passwords must be kept secure at all times. **Never** write them down and leave them where others can find them.
14. Passwords must be changed regularly: most Trust systems will enforce this. In future it is possible that a single (but strong) password will suffice to access all systems. Presently each system has its own password but a 'single-sign-on' facility can store these for each user and automatically enter the appropriate password at login.
15. Always choose strong passwords: preferably at least 8 characters and including a combination of upper and lower case letters (passwords are case-sensitive), digits, and other printable characters - but avoid spaces. Further suggestions are available in Guidance on choosing a password.

Smartcards

16. Trust 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 Choose-and-Book systems —where access to the Spine demographics is required —and by clinical staff accessing the network using the 'tap-and-go' system (see below).
17. 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 Datix.
18. 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.
19. 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

20. The Trust 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 the Trust, and staff are expected to monitor their accounts regularly. NHS staff are also eligible for accounts with the NHS Mail email system (addresses with the format user.name@nhs.net). Staff must only use ouh.nhs.uk or nhs.net for Trust business (i.e. not any other email system).
21. As NHS Mail accounts can transfer with users moving to other organisations, leavers must ensure that any Trust-related emails in their NHS Mail accounts are deleted (if necessary transferring them to an OUH account first).

22. 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. The Trust and NHS email systems should only be used for work-related messages.
23. Email should not be considered as a fully-secure medium. Users are responsible for ensuring correct addressing and appropriate content. Take especial care when forwarding or replying to messages.
24. Emails must not include patient or person-identifiable information (PID) unless strictly necessary and justifiable. Current NHS standards require such emails to be encrypted; presently only NHS Mail meets this standard for emails sent between NHS Mail users. It also has a system for encrypting messages and allowing recipients who do not have NHS Mail accounts retrieve them securely. It is permissible to send emails containing PID between Trust accounts (ouh.nhs.uk) but the sender is responsible for ensuring that the message is correctly addressed.
25. Emails may be sent direct to patients' 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, the NHS Mail secure facility (paragraph 24) should be used. All emails identifying patients **must** be filed in the patient's EPR record.
26. Emails containing patient-identifiable information must otherwise **not** be transmitted by any other email system or sent to addresses at other email systems.
27. Emails concerning Trust business and activities must reside on the central server (Exchange). If necessary for retention purposes, they may be transferred to approved file store. Contact information governance for details.
28. All email messages handled by the Trust's email system, together with emails created by staff on Trust business transmitted through other email systems (including NHS Mail) are the property of the Trust. They subject to the provisions of the Data Protection Act for subject access requests, and the Freedom of Information Act. The Trust may inspect any user's mailbox at any time for security reasons, to investigate possible breaches of this policy, or to fulfil a legal subject access request.

Internet use

29. Access to the public internet is provided for business use to support the Trust's patient care, education, training, and research, and to access information relevant to users' work.
30. The internet may be used for access to resources for personal use provided this does not interfere with the user's work or Trust business.
31. The Trust's Information Protection Policies apply equally to the use of the internet.
32. 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 Trust's Equal Opportunity and Harassment Policy. This includes hostile text or images relating to gender, ethnicity, race, sexual orientation, religious or political convictions and disability.

33. 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.

34. 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
1.4	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 (paras 24&25)
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

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 Trust business.
2. For the purposes of this policy, any reference to a mobile phone means smartphone, iPhone, Android, Windows or other mobile phone.
3. This document is a component of the Trust's Information Protection policy and should be read in conjunction with the parent policy and its components.

Scope

4. The policy applies to the following classes of device:
    - Smartphones (e.g. iPhone, Android phones, Windows phones, Blackberry phones);
    - Tablets (e.g. iPad, Android, Windows tablets);
    - Laptops/portable computers;
    - Portable memory devices (USB sticks and external hard drives/SSDs).
5. The policy covers both Trust and user-owned devices used for Trust activities/business.
6. The policy applies to all Trust staff (permanent, temporary, honorary) and to external contractors and anyone else using mobile devices for Trust purposes.

Criteria for the issue of a mobile device by the Trust

7. An employee may be eligible to have a mobile device issued by the Trust 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. IM&T Service will advise on the process for application and procurement via the Help Desk.

Use of personally-owned devices[1]

8. Staff are permitted to use their own devices for personal use provided that this does not interfere with the user's job, other staff, or the work of the Trust. Personal devices may connect to the Trust's guest wireless network (OUH-GUEST), from which access to the internet, including Trust and NHS email, is available, subject to the conditions of the Acceptable Use Policy.
9. Personally-owned devices may only be used for Trust business, or to store confidential information with the permission of the owner's Divisional General Manager (or Executive Director) and IM&T Services, who will assess the suitability of the device.

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

10. Users must comply with the following:
    - Personal devices may only be connected to the Trust's corporate network in exceptional circumstances when there is no practical alternative and connection is essential to the user's job. IM&T Services will assess the suitability of the device and install any software required to ensure secure use. In most instances connection to Trust services will only be permitted via virtual workspace software;
    - The device must have installed the latest version of the native operating system for the device, and this must be updated as and when new versions are released;
    - All devices must have Trust-approved anti virus software installed and active;
    - Any component of the device (e.g. charger) that is connected to the Trust's mains electricity supply has been checked for electrical safety in line with the relevant Trust policy;
    - All Trust IM&T and Information Governance policies (including this policy).

Acceptable use

11. Users of mobile devices must comply with the Acceptable Use Policy. Misuse of a mobile device connected to the Trust's networks will result in disciplinary action being taken and possibly confiscation of the device.

Mobile phones - safety issues

12. Staff must only use their phone when it is safe to do so. Since 1st 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 the Trust.
13. 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.
14. 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.
15. The Trust will accept no liability for the consequences of using a mobile phone (Trust or user- owned) whilst driving.

Security of mobile devices

Physical security

16. 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.

17. Loss or theft of any mobile device that connects to the Trust's corporate network must, in the first instance, be reported to IM&T Services (who will take action to locate and/or wipe the device remotely), and a Trust Datix incident form completed. For phones, the network service operator should also be informed.
18. 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

19. Mobile devices used to store person-identifiable data must be encrypted to the NHS standard, using AES256 with 256 bit or stronger keys.
20. Encryption to this standard is built-in to iOS devices but must be activated by setting a device passcode. This will be done automatically by IM&T Services for Trust-supplied devices and those that are permitted to connect to the corporate network (OXNET-WLAN). This is not required for connections to the Trust's guest network (OUH-GUEST).
21. Mac OS X devices are shipped with disk encryption software to NHS standards (FileVault) but this is not turned on by default and must be activated if the device is to connect to the Trust corporate network or store sensitive (e.g. patient-identifiable) data.
22. 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, IM&T Services can also store securely the key or access code.

Passwords

23. 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

24. File storage in 'the cloud' is increasingly popular as a means of synchronizing data between data devices and for backup. Services such as iCloud (Apple), OneDrive (Microsoft), Google Drive and Dropbox offer secure services but these are not necessarily safe, the main risks being associated with poor password management (by the user) and poor device security.
25. Whilst users of mobile computing devices may use cloud services to store/synchronise non-sensitive information they must not be used to store personal-identifiable data (PID) unless it has been specifically encrypted before transfer, if for no other reason that the Data Protection Act forbids transfer of personal data outside the EU and many cloud storage services are located outside the EU.

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 trust's 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 IG team.

Document History

Version	Date	Author(s)	Comment
1.2	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 document of the Information Protection Policy

Safe Haven Policy

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 Trust's Information Protection Policy and should be read in conjunction with the parent policy and its other components, and also the Confidentiality and Disclosure 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 Trust 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 anonymised or pseudonymised to maintain confidentiality.

Policy

8. All staff handling person-identifiable data for secondary uses (non-direct patient care) must follow the safe haven procedures below. Existing processes that are using patient identifiable information may need to be 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 the Trust 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 Disclosure policy.

Safe havens within the Trust

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 IM&T Services;
- pharmacies on all hospital sites;
- clinical secretarial and administrative offices.

Location/security arrangements

11. Safe havens should be located in areas that are locked and accessible via a coded key pad available and 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 should be stored in locked cabinets.

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 achieve registration by 31st December 2016.

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 and Disclosure component of the Information Governance Policy.

Further information

Trust policies and guidance

- Information Protection Policy
- Information Governance Policy
- Standard operating procedures for sharing information by telephone, post, and email.

External guidance

- Confidentiality. NHS Code of Practice (2003)

Legal framework

- The Data Protection Act 2018

Document History

Version	Date	Author(s)	Comment
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 Trust Policy Format / IGG review
1.0	March 2011		Approved by 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.
3. This document is a component of the Trust's Information Protection Policy and should be read in conjunction with the parent policy and its other components (notably the Safe Haven policy), and also the Confidentiality and Disclosure 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 living individual. "Identifiable living individual" means a living 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 General Data Protection Regulation and the Data Protection Act (2018).

Confidential patient data

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

   (a) the identity of the individual in question is ascertainable—

      (i) from that information, or

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

(ii) from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information, and

(b) 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 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 clinical audit, clinical correspondence, appointments and scheduling.

13. *Secondary use* includes all other uses, including research, commissioning, 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. **Anonymisation** makes re-identification impossible or at least very difficult. It involves the removal of all identifying characteristics, such as name, address, date of birth, 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

[2] For example, the Human Rights Act 1998, The Freedom of Information Act 2000, The NHS Act 2012 and associated legislation,

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

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 are 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 GDPR and the Data Protection Act treat pseudonymised data as personal data and so it remains subject to the same restrictions as the 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 Group of the Health Research Authority will set aside the requirement for consent 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 Records Management Code of Practice for Health and Social Care 2016.

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 sufficient 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) with access restricted to a need-to-know basis.

Pseudonymisation can be achieved by:

- removing patient identifiers;
- the use of the value ranges: for example, age instead of date of birth;
- by using a pseudonym.

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 to be used in place of NHS Numbers and other fields must be of the same length and formatted 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;
- pseudonymisation for external purposes must use different pseudonym values to any generated for internal use of the same dataset;
- data prepared for secondary use must only contain the data items that are required, pseudonymised as appropriate;
- pseudonymised data must be kept as securely as identifiable data.

Document History

Version	Date	Author(s)	Comment
2.1	July 2020	Dr Chris Bunch	Policies and procedures combined. Approved by IGDQG.
2.0d	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 Trust Policy Format / IGG review
Safe Haven and Pseudonymisation Policy 1.0	March 2011		Approved by 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 Trust's 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 in the Trust or at home.
4. All staff and contractors employed by the Trust must abide by this policy.

Policy

5. Staff (including contractors) working with confidential information must at all times ensure that:
    - 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;
    - confidential information is only printed if absolutely necessary;
    - before printing their default or chosen printer is correct;
    - 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;
    - paper documents containing confidential information are shredded or placed securely in confidential waste bins when no longer required;
    - 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;
    - desks and other workspaces are left sufficiently clear at the end of each working day to permit cleaning staff to perform their duties safely;
    - 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;
    - desktop computers and laptops are not left logged on when unattended: screens must be locked or the device closed down;
    - if sensitive or confidential information is visible to an unauthorised person standing in close proximity 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 Information Governance and Data Quality Group.

Document History

Version	Date	Author(s)	Comment
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 practice within the Trust. 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 Trust are subject to legislation which provides the patient with rights of confidentiality, protection against the unlawful processing of data and the right of consent.
3. The policy and accompanying guidelines set out the acceptable procedures for the Trust. 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 photography and video recording.
5. This document is a component of the Trust's 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. This policy applies to all recordings in the possession of the Trust including recordings originating from outside the Trust.
8. The policy applies to all Trust employees, staff with honorary contracts, contractors or guests who make recordings of patients in the course of their work.
9. All recordings are subject to this policy irrespective of who owns the equipment or the materials on which they are produced. Any breach of this policy may lead to disciplinary action.

Professional requirements

10. Doctors are bound by the General Medical Council's guidance *Making and Using Visual and Audio Recordings of Patients*.
11. Clinical photographers are bound by the Institute of Medical Illustrators' guidance *A Code of Professional Conduct for Professional Members (2014)*.

Policy

12. Anyone making recordings does so on the understanding that all recordings produced 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.
13. There are accompanying guidelines to this policy which must be followed.
14. Clinicians are responsible for gaining the patient's consent, explaining the recording procedure and explaining specifically how the subsequent recording will be used and distributed in the future. It is strongly advised that the forms in Appendix 3–6 of the *Patient Photography and Video Guidelines* are used to obtain written consent. This will form the lawful basis for taking, using and sharing images which identify individual subjects.
15. Photographic and video recordings may not be used for any purpose other than that covered by the original consent unless additional consent is obtained. Consent is required even when the patient is incidental to the main picture, e.g. documentation of equipment or procedures.
16. A patient has the right to withdraw consent at any time.
17. All recordings should be stored securely in the patient's medical record and be available for disclosure at the request of the patient or their representative.
18. Copyright in all recordings made by staff in the course of their work belongs to the Trust and must not be transferred.

Responsibilities

19. Oxford Medical Illustration is responsible for:
    - developing, reviewing and maintaining this policy and associated guidelines;
    - providing expert advice and guidance;
    - formally agreeing any exceptions. to the policy;
    - setting an example of good practice for all staff, ensuring compliance with the duties of consent, confidentiality and data protection.
20. **Divisional Directors, Divisional General Managers, Nurse Managers and Clinical Directors** are responsible for ensuring the distribution, communication, implementation of and compliance with the policy and guidelines the policy throughout their Division.
21. **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.
22. **Individual Trust staff** must familiarise themselves with the policy and guidelines before making recordings an comply with its requirements.

References

Relevant legislation

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)
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

Authors

Roddy McColl & Warwick Baggaley
Oxford Medical Illustration.

Document history

Version	Date	Author(s)	Comment
2.3	November	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	

Patient photography and video guidelines

Introduction

1. In this document the term "recording" is used to refer to a patient photography and video recording.
2. Any person making a recording does so on the understanding that all recordings produced will be subject to legislation, as listed in appendix 2, and 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. The GMC[1] and BMA[2] have issued specific guidance for doctors on making and using recordings.
3. These guidelines should be read in the context of the Patient Photography and Video Policy, a component of the Information Protection Policy.

Recordings made by Oxford Medical Illustration (OMI)

4. It is strongly advised that whenever practically possible, Oxford Medical Illustration's clinical photography and video services are used to make recordings. A continuous "no appointment" service for out-patients is offered from 8:30 to 12:30 and 1:30 to 4:30 each weekday. In-patients will be recorded either on the ward, in theatre, or in the department by arrangement, usually on the day of request.
5. A photographic studio and a video studio are located in the main OMI department on level 3 of the John Radcliffe. Photographic studios are also located on LG1 of the West Wing, Dermatology Outpatients at the Churchill and at the Nuffield Orthopaedic Hospital. The contact number for Oxford Medical Illustration is 01865 (2)20900, for clinical photography requests 01865 (2)23302 and for the NOC studio 01865 (7)38274.
6. Please refer patients using the Oxford Medical Illustration Clinical Photography Request Form, or the Oxford Medical Illustration Clinical Video Request Form (These forms should be completed in full by the referring clinician.

Recordings made by non-OMI staff

7. Where recordings are made by Trust staff other than Oxford Medical Illustration staff, the 'Consent to Clinical Photography — Non-Oxford Medical Illustration Staff' form, or 'Consent to Clinical Video — Non-Oxford Medical Illustration Staff' form should be used. Forms are available from the Oxford Medical Illustration intranet site. The bottom section of the form should be completed by the person taking the photographs or making the recordings as detailed below. This information is necessary should it be necessary to provide copies from the original files for legal purposes—for example, a request from a patient's solicitor.

Use of mobile phones

8. Only the Trust's clinical photography app, OUH FotoApp, should be used to take clinical photographs of patients. OUH FotoApp enables secure upload of images to Fotoweb, Trust's image management system, and Cerner Millennium EPR. It ensures all the necessary patient data is collected to enable safe storage and retrieval as well gaining the patient's consent to photograph. All other methods present a high risk relating to possible breach of patient confidentiality, data protection, patient dignity and privacy. Staff must not use any other method without express permission from the Caldicott Guardian. For more information and to register to use the app please go to the Clinical Photography intranet page.

Storage and retrieval

9. Whenever possible, recordings should be securely stored in the patients' records. If stored elsewhere there must be an effective audit trail to link the recordings to the correct patient records. All recordings should be treated as medical records and as such must be available for disclosure at the request of the patient or their representative (e.g. solicitor) for access to records, medico legal purposes or legal proceedings etc, if required.
10. To ensure such disclosure is possible digital files must be labelled, catalogued and securely stored in a manner that ensures retrieval is possible upon request. It is recommended that the patients MRN number and date of recording are incorporated into the filename or embedded as metadata in the image file.
11. Medical records and patients' access to them is governed by the Data Protection Act 2018 (living patients) and the Access to Health Records Act 1990 (deceased patients) as detailed in the OUH Health Records Management Policy.
12. The Trust follows the minimum retention period for health records as set out in the IGA Records Management Code of Practice (2016), Section 4. Photographic and video recordings should be retained for the period of time appropriate to the patient/specialty, this being a minimum of 8 years after the date of the patient's last attendance or date of death for non- specific care records. For specific care records, including children's records and mentally disordered persons, please refer to the code of practice.
13. Recordings on cameras should be uploaded and stored on a Trust computer as a matter of priority, shortly after recordings have been made.
14. Recordings and any associated personal information should be processed and stored safely to prevent accidental loss, unauthorised viewing or damage, in accordance with the Information Protection Policy.
15. Patient identifiable information (name, date of birth etc) must not be stored on any non-Trust owned computer, laptop, or mobile device under any circumstances.
16. Where possible, all digital recordings should be stored in their original format, without manipulation, to preserve their integrity. Proof of the integrity of the original may be required, for example, where photographic or video evidence is required in a court case.

17. Clinical photographic material must not be processed by commercial laboratories or agencies unless approved by the Trust. Contact Oxford Medical Illustration for advice.

Exempt images/recordings

18. The following types of recordings are exempt from the requirements for consent Level 1 and Level 2 on the consent form, provided any patient ID has been removed or redacted and they can be deemed non-identifiable:
    - 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.
19. It is nevertheless expected that the clinician responsible will inform the patient that recordings will be made, and ensure its documentation in the patient's records.
20. However, if a patient's condition—and hence the images obtained—are highly unusual or unique, it should not be assumed that the images are non-identifiable. In such cases, the patient's consent should still be obtained to use the images for non-clinical purposes.
21. All images in the patient record must be clearly annotated with unique identifiers e.g. name, DoB, MRN number. Where images are to be used for any other purpose other than patient care, for example training or publication, all patient identifiable information such as name, DOB, hospital number, or any other specific personal data that may lead to the patient being identified should be removed from all images before use. In the case of images being submitted for medico-legal purposes, it may be necessary to leave clear identification on the images. However, where images are considered intimate, in cases of sexual violence and abuse, only the MRN number should be used.

Consent

General principles

22. The following general principles apply to most recordings:
    - seek permission to make the recordings and get consent for any use or disclosure;
    - it is the responsibility of the clinician to seek informed consent from the patient. The 'photographer' (unless they are the clinicians themselves) is not responsible for obtaining consent;
    - give patients adequate information about the purpose of the recording when seeking their permission;
    - ensure that patients are under no pressure to give their permission for the recording to be made;
    - stop the recording if the patient asks you to, or if it is having an adverse effect on consultation or treatment;

- do not use recordings for purposes outside the scope of the original consent without obtaining further consent.
- consent is required even when the patient is incidental to the main picture, e.g. documentation of equipment or procedures or in the background of a film;
- all parties and projects undertaking recordings shall respect the dignity, religion, nationality and individual sensibilities of the patient;
- all parties and projects undertaking recordings shall be aware of and act appropriately upon the need for chaperones.

Levels of consent

23. The clinical photography and video request forms allow for three levels of consent:
    - **Level 1: Confidential Treatment Record.** Photographic or video recordings to be used in the patient's confidential treatment records only;
    - **Level 2: Restricted educational use.** In addition to level 1 consent, photographic and video recordings may be used for restricted educational use;
    - **Level 3: Publication.** Where clinical photographs or video recordings are required for publication or distribution in a journal, text book, DVD, website or any other open access medium a *'Photography Request for Publication'* or *'Video Request for Production and Distribution'* form must be used, detailing the name of the publication or production. Individual level 3 consent must be gained for each separate incidence of publication or for each production.

Documentation of consent

24. Where recordings form part of a clinical procedure (e.g. endoscopy), consent to the treatment provides consent to recordings for the purposes of the patient record. Patients indicating consent for procedures on the Trust standard consent to treatment forms are given, on those forms, the opportunity to document their agreement / refusal to recordings as part of their clinical procedure. It may be appropriate to use the 'Patient consent to Clinical Photography by non-Oxford Medical Illustration Staff' form or the 'Patient consent to clinical video recordings by non-Oxford Medical Illustration Staff' form in addition to this, particularly when the recordings may also be used for other purposes. Forms are available from the Oxford Medical Illustration intranet site.

25. When a recording is to be made by Oxford Medical Illustration staff, the 'Clinical Photography Request' form or 'Clinical Video Request' form should be used.

26. When a recording is to be made by non-Oxford Medical Illustration staff the 'Patient consent to Clinical Photography by non-Oxford Medical Illustration Staff' form or 'Patient consent to Clinical Video Recordings by non-Oxford Medical Illustration Staff' form should be used. On completion the form must be filed in the patients notes.

27. Consent documentation within the patient's medical record should include a summary of pertinent points of discussion and/or explanation, and any queries raised by the patient and how these were addressed if appropriate.

Photography and video recordings for clinical purposes

28. Where recordings are required for clinical purposes, the health professional carrying out the clinical procedure and recording is responsible for ensuring that the patient's consent is valid, i.e. informed, not made under duress, and that the patient has capacity to make the decision. It is the health professional who will be held responsible in law if the validity of consent is later challenged.
29. A full explanation of how the recordings will be used must be given to the patient before any photography or filming takes place. This must be documented in the patient's medical notes.
30. Written consent should be obtained and documented using the appropriate consent form, see above. The signed form should be filed in the patients' medical records.
31. Recordings which are made for treating or assessing a patient must not be used for any purpose other than the patient's care or the audit of that care, without the express consent of the patient or a person with parental responsibility for that patient. If you wish to use such a recording for education, publication or research purposes, you must seek consent in writing from the patient.

Photography and video recordings for non-clinical purposes

32. Where photography or video is for non-clinical purposes; namely, specifically for education, publication or research, written consent must be sought from the patient (or the person with parental responsibility).
33. The person seeking consent must ensure the patient is fully aware of the possible uses of the material, and the time period the usage will occur over, e.g. the next 6 months. In particular, the person must be made aware that it may not be possible to control future use of the material once it has been placed in the public domain.
34. Patients must know that they are free to stop the recording at any time and that they are entitled to view it if they wish, before deciding whether to give consent to its use. If the patient decides that they are not happy for any recording to be used, it must be destroyed.
35. If members of clinical staff are visiting the Trust for educational or research purposes and wish to take images for non-clinical purposes, the same requirements around consent apply. The member of staff taking the image should provide a clear audit trail of where the images will be stored and utilised, documented in the patient's case notes.
36. For photographs taken for the sole purpose of research, consent must be considered within the application for ethical approval. Further advice should be sought from the Trust's Research and Development Department.

37. Where external photographers and film companies are contracted by Trust, or where companies have requested access to photograph and film patients, staff or locations, the OUH Media and Communications Unit must be informed at the earliest possible stage. Staff must not sign agreements with companies or allow them to use their own model release/consent form without the express permission of the OUH Media and Communications Unit. For more information about policy for non-clinical filming and photography, please contact OUH Media and Communications Unit on x31471.

Photographic images for publication

38. Where photographic images are required for publication, including on a web site, a *'Photography Request for Publication'* form should be used. A separate form must be completed for each incidence of publication: the use of a blanket consent is not permitted. The form should be completed and signed by the patient/ parent/carer and one named author/clinician for any clinical photographs to be submitted for publication in a medical or scientific journal, DVD, web site, book, etc. The name of the publication and full title should be given, and the form signed and dated prior to submission. A copy of the form should be made for the patient and the original filed in the patients' medical records.

Video recordings for production and distribution

39. Where video recordings are to be incorporated in a production and distributed, including on a web site, a 'Video Consent for Production and Distribution' form should be used. A separate form must be completed for each production and the use of blanket consent is not permitted. The form should be completed and signed by the patient/parent/carer and one named clinician for any video recordings to be included in a production and distributed as a DVD, on website, etc. The name of the production and the extent of the distribution should be given, and the form signed and dated prior to release. A copy of the form should be made for the patient and the original filed in the patients' medical records.

Unconscious patients and emergency treatment

40. Unconscious patients and patients who need emergency treatment that cannot give their permission for the recording to be made, may be photographed or filmed as long as they are fully informed and their consent gained when capable. You must not use these images for any other purposes than immediate clinical care. When the patient regains capacity they must be informed that photographs have been taken and asked for their consent for further use. If the patient refuses consent to any form of future use then the recording must be destroyed. It must be noted in the patient's notes that the recording has been destroyed, the reason, by who and when.

41. If the patient is likely to be permanently unable to give, withholds consent for a recording to be made, or dies, you should consult with the patient's next of kin or seek permission from an individual acting under a Lasting Power of Attorney or a Court Deputy. You must not make any use of the recording that might be against

the interests of the patient. You should also not make, or use, any such recording if the purpose of the recording could be equally well met by recording patients who are able to give appropriate consent.

Still-births and post-natal deaths

42. Photographs of still-births and post-natal deaths may be requested by a consultant or midwife for grieving purposes/bereavement counselling. The consultant/midwife should seek the consent of the deceased's next of kin prior to taking the photographs. The mother will be given the opportunity to receive a copy. All photographs will be given to the parent at a pre-arranged time, at which occasion an appropriate healthcare professional / social worker must be present to offer appropriate support. If the parent does not wish to see any photographs, those taken must be destroyed, unless consent to retain them on file for future use is obtained.

43. If recordings of still-births or post-natal deaths are requested for clinical purposes the clinician must have written parental consent. Please refer to the Postmortem consent for a baby form

Children

44. Staff should consider very carefully the appropriateness of photographing or recording children. This should only occur where there is an agreed clinical need and this decision should be made by the child's consultant.

45. Recordings of children should be taken only if there are specific features that need recording for clinical reasons, e.g. assessing the progression of a skin lesion, suspected child abuse or teaching, e.g. an important clinical sign that might only be seen rarely.

46. Recordings should only include the specific areas of clinical concern. Whole body shots should only be taken if absolutely necessary.

47. Recordings of genital areas, or of the chest in peri or post pubescent girls, should only be taken in very exceptional circumstances – clearly defined by clinical need and in the child's best interests and this should be recorded in detail in the patient record justifying why such recordings are necessary.

48. It should not be assumed that a child under the age of 16 does not have the capacity to give consent in their own right. If you have any doubts about how to assess a child's capacity refer to the Department of Health's Reference Guide to Consent for Examination or Treatment.

49. If the child lacks capacity, then written consent from a parent or person with parental responsibility must always be obtained when undertaking clinical photography or video recordings of minors.

50. If a child does not wish an image to be used for non-clinical purposes, it must not be used, even if a person with parental responsibility consents.

51. Note: Parental responsibility may be assumed by the child's mother, biological father if married to the mother, adoptive parents, both parents in the case of divorce, or in loco parentis (e.g. teacher). Others may hold parental responsibility, but it may be appropriate to see formal evidence of this. If uncertain contact Legal Services for advice.

52. If the child reaches age 16 or if under 16, is assessed Gillick competent to consent in their own right during a course of treatment, consent from the young person must be obtained. If the young person does not consent to an image/recording to be used, it must not be used, even if a person with parental responsibility previously consented.

Incapacitated adults

53. Where adults lack the capacity to consent to a recording being taken for clinical purposes, it is lawful to take the recording for the purposes of care or treatment as long as it is in the patient's best interests to do so. In such circumstances, healthcare professionals should follow the procedures under the Mental Capacity Act 2005 and the associated Code of Practice, which includes consulting with family, friends or carers involved with the patient's care, or, where applicable, obtaining consent from an individual appointed under a Health & Welfare Lasting Power of Attorney (as above) or a Court Deputy.

54. Where healthcare professionals wish to take recordings of an incapacitated adult for research purposes, they may only do so if the research is related to the condition from which they are suffering. In such circumstances, healthcare professionals must follow the procedures under the Mental Capacity Act 2005 and the associated Code of Practice which includes obtaining approval from a Research Ethics Committee and consulting with family, friends or carers involved with the patient's care, or, where applicable, obtaining consent from an individual appointed under a Health & Welfare Lasting Power of Attorney (as above) or a Court Deputy.

55. Recordings of incapacitated adults for research or teaching purposes which are not related to the condition from which they suffer must not be taken.

Special circumstances

56. In very special circumstances where photographic and video evidence may be demonstrated to be beneficial to a patient's welfare or required for legal documentation, authorisation may be sought from the patient's Consultant, Clinical Service Lead, Senior Child Protection Clinician, or Child Protection Team. Examples of such instances are:

    - Suspected non-accidental injury to a child;
    - Visual evidence for legal reasons;
    - Persons obtaining treatment under false pretence;
    - Deceased patients whose next of kin is not known.

57. In the case of suspected non-accidental injury to a child, it is not always necessary to seek parental consent for the recording to be made. Children over the age of 16 are able to consent for themselves and children below the age of 16 may be able to consent to recordings if they have sufficient understanding and intelligence to understand fully what is proposed. If these circumstances do not apply, the child's treating consultant can authorise the recording if he or she believes that it is in the best interests of the child.
58. This list is not exhaustive, and it must be remembered that in all cases, photography and video sessions and the resulting recordings must be documented in the clinical notes.
59. If advice is needed on this issue, contact the Caldicott Guardian and, if applicable, the Trust's Child or Adult Protection lead.

Incidental recordings

60. In cases where the patient is incidental to a recording e.g. where the picture is to illustrate a particular equipment set up, consent to appear in the recording is still required from any patient or member of the public who feature in the recording.
61. Accidental recording of patients who have not given appropriate consent must be avoided. Images of a patient that have inadvertently picked up the images of another patient or patients who have not consented should not be published under any circumstances. Unless deleterious to the care of the subject patient, they should be destroyed.

Photographic and video material without consent

62. Photographic and video material for which there is no consent (e.g. material already in the teaching domain prior to the enactment of the Data Protection Act 2018) may be used for restricted teaching purposes i.e. within the Trust only, if the following conditions are met:
    - the patient cannot be identified from the photographic or video material;
    - appropriate attempts have been made to obtain retrospective consent.
63. You should not use any recording, from which a patient may be identifiable, for non clinical purposes if you cannot demonstrate that consent has been obtained for that use.
64. Where there is doubt concerning the continued use of specific images, the Caldicott Guardian/Legal department or Oxford Medical Illustration should be consulted.
65. Where a patient dies before consent is obtained, healthcare professionals should consult the deceased's next of kin or near relative and legal representative to ascertain whether they have any objections to the use of the deceased's personal data.
66. Where a patient has consented to photographic or video recordings but subsequently dies, healthcare professionals should consult the deceased's next of

kin or near relative and legal representative regarding any new use outside the terms of the existing consent.

67. Where pursuance of consent from grieving relatives is inappropriate, the image may only be used for the patient record. Confidentiality should be respected after a patient's death.

Copyright and confidentiality

68. Copyright in all recordings of patients made by staff in the course of their work belongs to their employing authority – Oxford University Hospitals NHS Foundation Trust.

69. All images and footage, when published (e.g. digital images on a website), must be accompanied with a copyright statement assigning copyright to Oxford University Hospitals NHS Foundation Trust, displaying the conventional copyright symbol and date taken. i.e. © Oxford University Hospitals NHS Foundation Trust 2015.

70. The Trust department Oxford Medical Illustration may use © Oxford Medical Illustration to enable them to track and manage the high volume of images they create.

71. Copyright in a clinical photograph or video recording should not be transferred, for example to a publisher, and it should be explicit in any publishing contract that copyright in the image or footage remains with the Oxford University Hospitals NHS Foundation Trust. Rights to publish can however be given, provided the appropriate consent has been obtained. These rights are normally subject to specific conditions e.g. a single publication, UK distribution only. Oxford Medical Illustration can provide advice on 'Licence to Publish'.

72. Copies of a recording may only be made with the permission of the clinician in charge and within the constraints of consent as laid out in this document. It must be noted in the patient's case notes that duplicate images and recordings have been made and where they are stored for audit purposes.

73. In the case of staff that leave the employing authority, recordings obtained during the course of their employment may continue to be used for teaching if appropriate consent has been obtained. If there is a requirement for photographs and footage to be published or released in any other way the permission of Oxford Medical Illustration must be sought first and the appropriate forms completed i.e. 'consent level 3: publication' form and 'consent level 3: production & distribution' form. Copyright in all clinical images remains with Oxford University Hospitals NHS Foundation Trust.

74. Breach of copyright materials or other failure to comply with current UK legislation with regard to data protection is an offence punishable by law.

75. Note that passing material to colleagues for internal use is permitted (e.g. for use in seminars, presentations, etc). However, you should be aware that sending images via email is an insecure method without encryption.

Access to Health Records

76. On receipt of a request for copies of health records under the Data Protection Act 2018 (living individuals) and the Access to Health Records Act 1990 (deceased individuals), colour photocopies of any clinical photographs will be supplied. The normal fees for providing access to health records under these regimes will apply. Should the patient require high quality copies of any photograph then additional charges may apply.

Further reading

1. General Medical Council. (2002). Making and using visual and audio recordings of patients. London: GMC.
2. British Medical Association (2018). Taking and using visual and audio images of patients. London: BMA.
3. Information Governance Alliance (2015). The Use of Mobile Devices in Hospitals. Leeds: IGA
4. The Data Protection Act, (2018).
5. The Access to Health Records Act, (1990)
6. Information Governance Alliance (2016). Records Management Code of Practice for Health and Social Care 2016. Leeds: IGA
7. Royal College of Paediatrics and Child Health. (2009). Guidance for best practice for the management of intimate images that may become evidence in court. London: Faculty of Forensic and Legal Medicine.
8. Department of Health. (2009). Reference Guide to Consent for Examination or Treatment. London: Department of Health.
9. Mental Capacity Act, (2005).
10. Department for Constitutional Affairs (2007). Mental Capacity Act 2005 Code of Practice. London: Department for Constitutional Affairs
11. The Copyright, Designs and Patents Act, (1988)

Acknowledgements

British Photographers Liaison Committee. ABC of UK Photographic Copyright 1994.

Institute of Medical Illustrators, “Code of Professional Conduct,” June 2008.

Institute of Medical Illustrators precedent "Photography and Video Recordings of Patients: Confidentiality and Consent, Copyright and Storage" Policy.

Addenbrooke’s NHS Trust, “Photography and Video Recordings of Patients : Confidentiality and Consent, Copyright and Storage,” November 1999.

University Hospital Birmingham NHS Foundation Trust: Photographic & Video Recording Consent and Confidentiality Policy.

Birmingham Children's Hospital NHS Foundation Trust: Clinical Photography of Patients: Policy on Confidentiality, Consent, Copyright and Storage.

Authors

Roddy McColl & Warwick Baggaley, Oxford Medical Illustration.

Version control

Version 2.3	May 2019	Updates to Appendix 1
Version 2.2	August 2018	Updated for Data Protection Act 2018 compliance
Version 2.0	December 2013	
Version 2.1	January 2016	
Version 2.2	November 2018	

Revision due

August 2021

APPENDIX 1: Useful Contacts within the Trust

Chief Nurse	Sam Foster	x26889
Trust Caldicott Guardian	Dr Christopher Bunch	x21343
Information Governance Manager	Nuala Buchan-Brodie	x26912
Senior Information Risk Owner	Sara Randall	x72700
Library Development Manager (Health Records)	Daniel Lightfoot	x26304
Head of Oxford Medical Illustration	Roddy McColl	x20900
Research Governance Manager	Jo Franklin	x72238
Head of Research and Development Operations	Chris Bray	x23591
Director of Communications	Matt Akid	x72984

APPENDIX 2: Relevant Legislation

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) Mental Health Act 1983 and 2007

Mental Capacity Act 2005

Obscene Publications Act 1956 & 1964 Copyright & Patents Act 1988

Human Rights Act 1998

Professions Supplementary to Medicine Act 1960

Freedom of Information Act 2000

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 the Trust. 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 digital 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 Information Protection Policy.

Policy

4. The smartcard registration process is operated locally by the Trust Registration Authority (RA), a Trust department which is required to conform to national registration policy and procedures. 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] and to all staff members using a smartcard.

Registration procedures

ESR/RA link

6. 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 Care Identity Service (CIS) system.
7. Role based access control (RBAC) will be maintained by the RA Manager and approved through the Information Governance and Data Quality Group (IGDQG) on a regular basis. If required, RBAC definitions may be amended at any time for operational purposes without the reference to IGDQG but any changes will be notified to the group as soon as possible afterwards;
8. 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

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

completed by the requesting manager and sent by internal email to smartcards@ouh.nhs.uk.

New starters

9. The Human Resources (HR) department will notify the RA Office of all new staff and their start date.
10. The RA Office will register all staff who are required to use the Cerner electronic patient record (EPR) as a matter of course, whether they will need a smartcard or not.
11. In order to register, new staff members must bring suitable forms of identification[2] to the RA Office.
12. The RA office will apply to Information Management and Technology Services for network and email accounts for new starters so that they are available on their induction day.
13. 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.
14. All users will be associated in ESR/CIS and photographs uploaded into the active directory folder.
15. The RA Office will set up new clinical staff to use the virtual work-stations.
16. 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.
17. 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.

Leavers

18. The HR Department will notify the RA Office monthly of staff that are due to leave. Departmental managers must also to notify the office of any leavers within their departments.
19. The RA Office will deactivate or update leavers' role profiles in CIS as soon as practicable after they leave or before, and will notify IM&T Services to deactivate their network/email/SEND accounts.
20. 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

[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.
[3] See also the Acceptable Use policy.

smartcards destroyed. Staff leaving the work in a local NHS Trust can continue with the same smartcard but the roles within the OUH CIS will be revoked.

Revocation of smartcards

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

    21.1. The smartcard is lost or stolen

    21.2. There has been some other security breach associated with the smartcard or smartcard certificate

    21.3. The user is no longer employed by an NHS organisation

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

Lost/stolen or damaged smartcards:

23. 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 DATIX before a new card can be issued.

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

Smartcard passwords

25. Users will be required to enter a smartcard password when collecting their cards.

26. 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.

Locums, agency and bank personnel:

27. The following points should be considered:

    27.1. Staff working as part of a team may not require a smartcard to fulfil their role;

    27.2. Some staff may already have been registered and will only require a role profile added;

    27.3. 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.

28. 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:

28.1. 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;

28.2. The required ID documentation has been seen;

28.3. 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;

28.4. Should the temporary staff member change department, a new RA02 form will need to be completed by their new line manager;

28.5. 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.

29. This staff group includes:

- locums
- NHS Professionals
- Clerical agency staff
- Agency staff for AHP and other groups

Training for staff

Medical staff and students

30. 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 Management System and emailed regarding the required training.

31. This process also applies to medical students before receiving an active smartcard.

All other staff:

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

Short term access (Tenens) cards:

33. 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.

34. The Tenens system is maintained by IM&T Services and is closely monitored by the RA manager. Regular audits are completed and departments notified via email of any required actions.

35. Lost or stolen smartcards not returned will only be replaced once an incident form has been completed.

Local Support

36. 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

37. 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.

38. 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

39. 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
2.6	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