Information Governance Policy

Category	Policy
Summary	Main policy document for Information Governance
Equality impact assessment	February 2015. Reviewed June 2023
Valid from	Once approved
Date of next review	July 2026
Approval date	3rd August 2023 at Trust Medical Executive (TME)
Distribution	All staff
Related documents	Component policies as listed on pages 2–3 .
Author	Dr C Bunch, Data Protection Officer
Further information	
This document replaces:	Information Governance Policy v9.2

Lead Director: Chief Digital and Partnership Officer

Issue Date: 03/08/2023

This document is uncontrolled once printed.

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

Introduction

1. Information is a key asset, both for clinical care and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.
2. Information governance is a broad framework for ensuring and assuring that information is managed lawfully and securely, and that the confidentiality of personal and sensitive information is maintained appropriately. It encompasses information protection and risk management, confidentiality freedom of information, access to and sharing/disclosure of information, records management and the governance of information technology (IT) and IT projects.
3. Robust information governance requires clear and effective management, accountability structures, processes, policies & procedures, trained staff, and adequate resources.
4. Oxford University Hospitals NHS Foundation Trust (OUH) is the Data Controller for personal data as specified by data protection legislation and is registered with the Information Commissioner's Office (ICO) with registration number ZA152461.
5. This is one of three over-arching policies covering information governance. The other two are the Information Protection Policy and the Records Policy.

Background/Scope

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

Key Updates.

8. General updates to keep up with national requirements.

Aim

9. Compliance with national and legal requirements.

Policy

10. All employees and parties must maintain the highest standards in all matters concerning the use, handling, protection, transmission and sharing of personal information held by OUH, and must at all times act lawfully and take note of the guidance set out in this policy and its accompanying documents.
11. This Policy document comprises this document and the attached component policies, which are also available separately:

Information Governance Framework: sets out the arrangements for the management and implementation of information governance at OUH.
Confidentiality and disclosure: balancing the the duty of confidentiality and duty to shre data appropriately and safely.
Freedom of information and environmental information: compliance with statutory obligations.

Subject access requests (SAR) and SAR procedures: respecting the rights of data subjects.
NHS number: the primary patient identifier.
Data quality: ensuring that data is accurate and relevant.

Review

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

References

- Data Protection Act (2018) as updated June 2023 (includes the UK GDPR).
- Freedom of Information Act (2000)
- Human Rights Act (1998)
- Access to Health Records Act (1990)
- Care Act (2014)

Document History

Date of revision	Version number	Author(s)	Reason for review or update
Aug 2023	9.3	Dr C Bunch Data Protection Officer Ralph Shackell Information Governance Manager	Approved by TME 03/08/2023
Jun 2023	9.3d	Dr C Bunch Data Protection Officer Ralph Shackell Information Governance Manager	General updates and corrections;. Incorporation of additional component policies. New format
Nov 2017	9.2	Dr C Bunch Data Protection Officer Nuala Buchan-Brodie Information Governance Manager	Minor updates for consistency with the GDPR
Nov 2016	9.1	Dr C Bunch Caldicott Guardian Nuala Buchan Brodie IG Manager	Minor updates and corrections and to include pseudonymisation and clear desk policies
Apr 2014	9.0	Dr C Bunch Caldicott Guardian	Updated and converted to IG policies format

Consultation schedule

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

Endorsement

Chief Digital and Partnership Officer (CDPO)

Appendix 1: Responsibilities

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

Appendix 2: Definitions

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

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

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

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

Appendix 3: Education and Training

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

Appendix 4: Monitoring compliance

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

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

Appendix 5: Equality Impact Assessment

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

The Information Governance Framework

Introduction

1. This framework sets out the arrangements for the management and implementation of information governance throughout the Oxford University Hospitals NHS Foundation Trust (OUH).

2. This document is a component of the OUH Information Governance Policy and should be read in conjunction with the parent policy and its components.

Scope

3. This framework covers all OUH sites and areas and all who work in them and handle information, whether or not OUH employees.

4. Information governance (IG) comprises the following key areas:

    - governance, compliance and assurance;
    - data security, protection, and risk management;
    - confidentiality, information sharing and disclosure;
    - freedom of information and subject access to records;
    - records management;
    - quality assurance;
    - data security and protection training.

Governance, compliance and assurance

People

5. The *Senior Information Risk Owner (SIRO)* is responsible and accountable for information risk management processes and associated policies. The SIRO at present is David Walliker.

6. The *Caldicott Guardian* oversees and advises on the confidentiality, handling, sharing and disclosure of personal identifiable information. The Caldicott Guardian at present is Dr Alastair Moore (Interim).

7. The SIRO and Caldicott Guardian are accountable to the Chief Executive for their information governance responsibilities.

8. *Deputy SIROs* have accountability and responsibility for information risk and the application of information risk management processes and associated policies at Divisional level, and are accountable in this role to the SIRO.

9. The *Data Protection Officer* provides advice on data protection and monitors compliance with the UK General Data Protection Regulation ((UK GDPR) and the Data Protection Act (2018). The Data Protection Officer at present is Dr Christopher Bunch.

10. The *Head of Information Governance* is responsible for supporting and monitoring the implementation of this policy, and is accountable to the SIRO. The post is currently held by Ralph Shackell.

11. The *Information Governance* and *Freedom of Information (FOI) Officers* support and are accountable to the Head of Information Governance, with general responsibility for information governance matters and freedom of information. The Information Governance at present are Robin Peach-Toon, and Jenny Kitovitz; the FOI Officer is Matthew Schnelting.

12. The Information Governance Manager and the Information Governance and Freedom of Information Officers comprise the Information Governance Team, and can be contacted at information.governance@ouh.nhs.uk.

13. The *Director of Digital Services* is accountable for the provision, management and governance of OUH's major information technology (IT) systems. The Director of Digital Services at present is Matt Harris.

14. The *Data Quality Manager* is accountable for all aspects of data quality and audits. The post is presently vacant.

15. Information governance is everyone's responsibility, and all staff must be aware of and work within this framework, and comply with related policies.

16. Each Division should have an information governance lead who provides liaison between their Division and the Information Governance team, and who attends relevant Information Governance and Data Quality meetings.) IG leads are also expected to take ownership of, and seek to improve, the quality of information and its management within their service.

The Information Governance and Data Quality Group (IGDQG)

17. The Information Governance and Data Quality Group (IGDQG) is the primary body overseeing and supporting information governance within OUH, ensuring compliance with statutory responsibilities, legal obligations in terms of confidentiality and data protection, and that information is effectively managed within these policies and framework.

18. Its purpose is to support and drive data quality, protection and governance, ensuring that OUH complies with statutory responsibilities, fulfils its legal obligations in terms of confidentiality and data protection, and manages high quality information efficiently within a robust governance framework.

19. IGDQG reviews information governance, data security and data quality audits and reports, and progress with the annual Data Security and Protection Toolkit self-assessment. Meetings are heldbi-monthly or as required.

20. IGDQG is chaired by the Caldicott Guardian, and reports to the OUHAudit Committee.

21. Membership[1] includes the Caldicott Guardian and Senior Information Risk Owner, the information governance team, Chief Clinical Information Officer, representatives from IM&T services, finance, resourcing, training, health records, clinical coding, and the divisional information governance leads.

Information assets

22. An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. The information may be statically stored, or in transit ('data flow'). Key information assets, including all assets which include person-identifiable information, must each have an information asset owner and, optionally, an asset manager.

23. *Divisional Directors of Operations* have devolved SIRO responsibilities for information assets within their division.

24. *Information asset owners (IAOs)* are responsible for documenting and registering their information assets and data transfers, and for ensuring their security.

25. IAOs must undergo approved training for their role before assuming responsibility and will be accountable in this role to their divisional director of operations (in their Deputy SIRO role).

26. *Information asset managers (IAMs)* may be assigned day-to-day responsibility for each information asset to support the IAO.

27. All information assets and transfers that concern person-identifiable information must be recorded on the OUH online information asset register (IAR). Details will include the nature and purpose of the asset, information held, its location, owner, security arrangements, disaster recovery arrangements, the destinations and sources of any transfers of information into or out of the asset, the legal basis for processing, and an assessment of the risks to privacy. Much of this information will be contained within a Data Protection Impact Assessment (see below).

Data protection impact assessments

28. A 'privacy-by-design' approach is required for all systems and processes that involve the processing of personal data.[2] The information governance team or the Data Protection

[1] The full membership list and terms of reference are available on the information governance intranet pages.
[2] UK GDPR Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier

Officer should be consulted during the conception and design phase of any new information asset, service, system or process involving personal data, and *before* any procurement process is undertaken.

29. A *Data Protection Impact Assessment* (DPIA) is legally required if the processing "is likely to result in a high risk to the rights and freedoms of natural persons".[3] This is the case when confidential patient information is involved and may be so for data concerning members of staff, especially if special category data[4] is involved.

30. At a minimum the UK GDPR requires a description of how the data will be used, an assessment of 'proportionality' - i.e that the use of personal data can be justified and only the minimum necessary is used; an assessment of the risks to the rights and freedoms of those whose data is being used; and the measures that will be employed to mitigate those risks.

31. The DPIA must be undertaken at the start of any project or plan to introduce a new (or make a substantive change to an existing) information asset, data flow, service, system or process, using the DPIA template available from the Information Governance intranet.

32. DPIAs are the responsibility of the Data Controller, in this case OUH, and should be completed by the relevant information asset owner or project lead. The Information Governance team, Data Protection Officer, and Caldicott Guardian are available to advise and help as required.

33. The DPIA should cover all processes involving personal data, including for example: identifying data subjects, extracting data on the from systems or entering data into them, de-identifying or otherwise transforming the data, and sharing it with third parties.

34. Where the project involves a third-party system, the supplier is obliged to provide help and support to the DPIA process (generally by supplying the necessary technical information) but should not be expected to complete the entire form.

35. There is no formal requirement for DPIAs to be 'signed off', but completed forms must be sent to Information Governance for review.

36. A DPIA is a dynamic process throughout the life of a project: it should be updated if any circumstances change, and reviewed at least annually.

The Data Security and Protection Toolkit (DSPT)

37. Each year, NHS organisations must report centrally to NHS England on their implementation of standards set out in a national toolkit, the Data Security and Protection Toolkit. This covers a comprehensive set of data security and information

or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

[3] UK GDPR Article 35(1).

[4] Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

governance standards, provides evidence of their implementation, records compliance with the law and national guidance, and demonstrates whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

38. Compliance with the toolkit and adequacy of submitted evidence will be audited by OUH's internal auditors.

Information-related incidents and reporting

39. All staff are expected to report, via the incident reporting system (Ulysses), any actual or potential incidents involving information. The UK GDPR requires that breaches of personal data are reported within 72 hours. Examples of the types of incidents that should be reported include:

    - breaches of confidentiality or inappropriate release of information;
    - failures of communication regarding a patient, e.g. with the patient, relatives or between staff or departments;
    - information security related concerns.

40. Incidents must be graded according to the significance of the breach and the likelihood of those serious consequences occurring using the grading matrix in the DSPT's Guide to the Notification of Data Security and Protection Incidents. (2018). The Information Governance team will notify data breaches that meet the threshold for reporting centrally via the DSPT. Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor, the incident is reportable and full details will be automatically be transmitted from the DSPT to the ICO and the NHS Digital Data Security Centre. The DHSC will also be notified where it is (at least) likely that harm has occurred, and the impact is at least serious.

41. The SIRO, Caldicott Guardian and the Data Protection Officer must be informed immediately of any incident involving the unauthorised disclosure of personal data. IGDQG will monitor and review all such incidents and ensure remedial and preventative measures are/have been taken.

Audit

42. The internal auditors will undertake annual assessments and/or audits of:

    - compliance with legal requirements;
    - implementation of information governance standards and the DSPT;
    - information and IT security arrangements.

Privacy notices

43. A privacy notice informing patients of how information about them is collected and used must be published in accordance with the UK GDPR. This must clearly be signposted on every page of any website that carries the OUH brand, and will also be available through the OUH Intranet, information leaflets, and posters displayed at patient reception points.

44. Staff will be provided with a privacy notice detailing how information collected about individual staff members. Is used

External contractors

45. Third parties including contractors, temporary agency staff, honorary staff and PFI staff may need access to information assets such as telephones, computers, paper and electronic records. This poses an information risk and requires that steps are taken to ensure that assets are accessed and handled correctly.

46. The procurement department is responsible for the monitoring and review of contracts for external contractors to ensure that any relevant data security and protection standards are included and met, any issues that arise are resolved, and any foreseeable risks are mitigated. The department will maintain a register of third-party contractors.

47. Particular care must be taken when contractors sub-contract, i.e. create a supply chain. The security of any chain is determined by its weakest link, so due diligence must be applied to the entire chain.

48. Impact assessments to evaluate any potential threats to networks, systems and locations from third party workers will be required to identify and mitigate risks. For example, it may be necessary to restrict access to certain systems.

49. The NHS standard contract templates cover the most important data protection aspects, but additional clauses or a separate data processing agreement may be necessary to mitigate any identified risks. Terms and conditions must make clear that any failure to uphold information governance standards will be at the contractor's risk.

Information protection, security and risk management

50. The Information Protection Policy and its component policies (acceptable use, network security, mobile devices, patient photography and video, safe havens and registration authority) are designed to ensure effective and secure management of its information assets and resources, and of the flow of information into and out of the organisation.

51. OUH Digital (IM&T) Services has responsibility for cyber security, supported by a cyber security analyst and task force.

Confidentiality, information sharing and disclosure

52. OUH regards all identifiable personal information relating to patients and staff as confidential except where the law or national policy requires otherwise.

53. OUH is the custodian and controller of a vast amount of sensitive data from patients and staff to whom it owes a legal duty of confidence. At the same time, it has a duty to share patient information appropriately and safely to support their care. In discharging these responsibilities staff are expected to abide by the law and the Caldicott Principles. These

are covered in the accompanying component policy for confidentiality and information disclosure and the Information Protection Policy.

54. The Caldicott Guardian is responsible for advising OUH and its staff on matters relating to confidentiality, information sharing and disclosures of confidential patient information.

Freedom of information and subject access requests

55. The Freedom of Information Act 2000 (FOA) provides members of the public with a general right of access to information held by public authorities, supporting openness and transparency across the public sector, and promoting a greater understanding of how public money is spent, and how decisions are taken which affect the services provided by public bodies.

56. Similarly, the Environmental Information Regulations 2004 (EIR) provide public access to environmental information held by public authorities.

57. Freedom of information and environmental information are both covered by the Freedom of Information and Environmental Information Regulations policy component of the Information Governance policy.

58. Subject access requests are covered by the Subject Access Request Policy component of the Information Governance Policy, of which this policy is a component.

59. Requests related to medical records are handled by Legal Services, for occupational health matters by the Occupational Health Department, for sexual health matters by the sexual health service, for radiology images by IM&T Services, and for CCTV images by the security services.

Quality assurance

60. The quality of information and data is key to its effective use and management. Managers will be expected to take ownership of, and seek to improve, the quality of data collected and held within their services.

61. Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

62. The OUH Data Quality Policy provides the framework for information quality assurance from its point of collection or acquisition, and through any subsequent use.

63. Assurance will be monitored by the Information Governance and Data Quality Group and provided to the Trust Board via the Audit Committee.

Training

64. All staff must undertake annual basic data security and protection training. Staff handling patient information must also undertake additional training at a level commensurate with their role and as defined by the Information Governance Training Needs Analysis. Face-to-face training sessions will be arranged for staff who do not have access to online training.

65. Comprehensive, graded information governance training is available online for NHS staff nationally. Additional training required will be determined by a training needs analysis. Management and monitoring of training will follow the OUH Learning and Development Policy. This information can be accessed via the Learning and Development pages on the OUH intranet.

Document history

Date of revision	Version number	Author(s)	Reason for review or update
August 2023	v3.5	Dr Chris Bunch Data Protection Officer	Approved by TME 03/08/2023
June 2023	v3.5d	Dr Chris Bunch Data Protection Officer	General update and corrections
Sep 2021	v3.4	Dr Chris Bunch Caldicott Guardian	General update and corrections
Mar 2018	v3.3	Dr Chris Bunch Caldicott Guardian	Minor corrections
Jan 2018	v3.2	Dr Chris Bunch Caldicott Guardian	Updated for GDPR
Mar 2017	v3.1	Dr Chris Bunch Caldicott Guardian	Updated IAO section
Nov 2016	v3.0	Nuala Buchan Brodie Information Governance Manager Dr Chris Bunch Caldicott Guardian	Rewritten as a component of the Information Governance policy

Confidentiality and Disclosures Policy

Introduction

1. NHS organizations and those carrying out functions on behalf of the NHS have a duty of confidence to patients and a duty to support professional ethical standards of confidentiality. This duty is conferred by common law[1], statute[2], contract of employment, and professional registration.
2. The use of confidential personal information should always be consistent with the eight *Caldicott Principles*.
3. Anyone working for or with the NHS may record, handle, store or otherwise come across information that is capable of identifying individuals. All have a personal duty of confidence to those individuals.
4. This policy is primarily but not exclusively concerned with the confidentiality of patient information. It applies also to information regarding other individuals, including staff, where confidentiality is expected.
5. Alongside the duty of confidentiality is a duty to share information when it is necessary for or appropriate to do so in the best interests of patients' clinical care.
6. This document is a component of the Information Governance Policy and should be read in conjunction with the parent policy and its other components.

What is confidential information?

7. Confidential information is information entrusted by an individual in confidence, when there is a general obligation not to disclose that information without the individual's consent, for example in a doctor/patient relationship. It may include personal information such as name, age, address, and personal circumstances, as well as sensitive information regarding health, race, sexuality, etc.
8. Confidential information may be known by individuals, and/or stored on any medium. Photographs, videos etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally.
9. *Person-identifying information (PID)* (i.e. that which identifies individuals personally) is assumed to be confidential and should not be used unless absolutely necessary. Whenever possible, *anonymised data*—from which personal details have been removed and which therefore cannot easily identify the individual—should be used instead. Note however that even anonymised information can only be used for justifiable purposes.

[1] The common law duty of confidentiality.
[2] Principally the Data Protection Act (2018) which incorporates the UK General Data Protection Regulation.

Awareness and compliance

10. Everyone must be aware of the importance of confidentiality, and their responsibilities for maintaining confidentiality and keeping information secure.
11. Staff must comply with the requirements of the current data protection legislation, Caldicott principles, the NHS Confidentiality Code of Practice, and the Information Protection Policy, of which this is a component.
12. Where it is necessary or appropriate to share information with others, this must be done lawfully and in line with guidance referred to in this document. Further advice may be obtained from the Caldicott Guardian.
13. Breaches of confidentiality are a serious matter. Failure to comply with this policy may result in disciplinary action being taken. No employee shall knowingly misuse any information or allow others to do so.

Acting on the duty of confidentiality

14. Personal information, given or received in confidence, must only be used lawfully. In the healthcare setting, the Data Protection Act allows the use of patient information for their direct individual care and for certain aspects of managing and assuring its delivery. Other uses (often called 'secondary' uses) will generally require consent as a legal basis unless required by statute, overriding public interest or other legal directive such as a court order (see next section).
15. Even where there is a legal basis for using and sharing information other than consent, there is a legal requirement for transparency, i.e. that individuals are fully informed of the uses to which information collected about them will be put. This will be covered in part by the Trust's published privacy notice, but staff also have a duty to inform patients when they wish or intend to share or disclose information about them.
16. No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information. This is usually the patient but sometimes another person (e.g. relative or carer) may be the source.
17. Patients have the right to object to the use of their personal health data for purposes other than their individual care. All such objections must be recorded and respected[3].
18. The duty of confidence is generally accepted to extend after death, in contrast to data protection legislation which applies only to living individuals.

[3] Patients have been able to register their wish to opt out of the use of their information for secondary uses from May 25th 2018 via the National Data Opt-out. Providers will have to respect any opt outs from October 2021.

19. The duty of confidentiality is not absolute: in some circumstances, such as safeguarding, the 'duty to share' can be as or more important as the duty to protect confidentiality.

Disclosure of confidential information

20. When information is passed from one to another, it is said to have been *disclosed* to the recipient. Good practice in maintaining confidentiality is mainly about ensuring that patients are aware when and why disclosures occur, and that such disclosures are necessary, appropriate, and undertaken safely and securely.

21. In many situations it may not be strictly necessary to disclose the identity of the patient. For example, it is often sufficient to communicate or discuss just the clinical details in order to obtain advice about management of a particular patient.

Inappropriate disclosure

22. Inadvertent or inappropriate disclosure of confidential information is potentially a serious matter. Adherence to the following principles will reduce the risk of this occurring.

    - assume information is confidential unless you are certain it is not;
    - whenever possible, remove person-identifying details (e.g. name and address);
    - do not give out information unless you are certain that the requestor has a right to receive it. Be especially careful on the telephone: always check the identity of the caller and the individual about whom they are enquiring. Do not automatically assume that they have a right to the information;
    - do not talk about confidential matters where you can be overheard, e.g., near another patient, in the queue at the canteen, in a lift, etc. Be careful not to leave or inadvertently display confidential notes in public places;
    - ensure that clinical records, computer screens and other confidential material cannot be viewed by unauthorized persons;
    - when sending confidential material to another location, always ensure that it is securely packaged;
    - always dispose of confidential material by the proper means. Papers must be put in designated confidential waste bags or bins.

Relatives and friends

23. Patients will usually expect close relatives to be informed about their diagnosis and care, but this may not always be the case and relatives and friends *do not have an automatic right to any information* about a patient without that patient's consent.

24. In the case of patients with capacity it is important that staff discuss with the patient with whom they are happy that information about their condition may be shared. In the case of patients who lack capacity to consent to this, staff should

normally act in the patient's best interests, and it may be appropriate to involve one or more close relatives or friends. The substance of such discussions should be documented in the patient's records, and regularly reviewed and updated.

Disclosure in the public interest

25. Disclosure of personal information without consent may be justified where failure to do so may expose the patient or others to risk of death or serious harm. The patient should normally be informed before disclosure.

Statutory and mandatory disclosures

26. Disclosure may be required in the following circumstances:

Circumstance:	Disclosure By:	Disclosure To:
Notifiable infectious diseases	Doctor currently responsible for patient's care and welfare	Local authority or local Health Protection Team
Poisonings and serious accidents at the workplace	Doctor currently responsible for patient's welfare	To the Health and safety Executive.
Abortions	The doctor who terminates the pregnancy	To the DHSS Chief Medical Officer on form HSA4
Births	Member of staff attending the birth	Child Health Department on Form SP7198 CH1 – Notification of Births
Road Traffic Accidents	Emergency department medical staff	There is no duty of disclosure except if an offence of death by dangerous driving may have been committed, or to obtain payment for treatment. The police must obtain the doctor's consent before obtaining a breath or blood specimen from a suspected patient.
Police requests	Medical team or Legal Services	Request must be made by a senior officer in writing giving the nature of the information sought and the legal justification. If in doubt contact the Caldicott Guardian.

Bodies empowered to order disclosure include:

- A Court of Law (including Coroners Court and Industrial Tribunals)
- The Parliamentary and Health Service Ombudsman
- Inquiries appointed by the Secretary of State
- Health and Safety Executive
- Employment Medical Advisory Service
- Health professions' registration bodies – doctors, dentists, nurses, midwives, health visitors, opticians, allied health professionals, pharmacists.
- Mental Health Act Commission
- Mental Health Tribunals

27. **Disclosures to non-NHS organisations** such as social services may be essential to the continuing care of the individual but must be strictly controlled.
28. **Additional categories:** Confidential information should **not** be disclosed to the following agencies unless in exceptional circumstances, or with the consent of the patient:
    - Department of Social Security (DSS / Benefits Agency). The patient's consent must be obtained before notifying the Benefits Agency of their stay in hospital.
    - Employers
    - Schools
    - Police (unless in conjunction with prevention or detection of serious crime: e.g. treason, murder, manslaughter, rape, kidnapping, certain sexual offences, causing an explosion, certain firearms offences, hijacking, causing death by reckless driving, offences under prevention of terrorism legislation).

Responsibilities

29. The Caldicott Guardian is responsible for overseeing and advising on issues of confidentiality and information protection for the Trust.
30. Managers are responsible for ensuring that all staff, including temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information.
31. All staff are responsible for adhering to this Policy and following the associated guidelines, and for safeguarding the confidentiality of all personal and Trust information, transmitted or recorded by any means.

Additional information

External guidance

- Confidentiality. NHS Code of Practice (2003)
- GMC: Disclosing patients' personal information: a framework
- To Share or Not to Share. The Information Governance Review
- The Information Commissioner's Office code of practice on data sharing
- Striking the Balance: Guidance on information sharing

Legal framework

- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Human Rights Act 1998
- Public Information Disclosure Act 1998

Document History

Version	Date	Author(s)	Comment
3.3	August 2023	Dr Chris Bunch Data Protection Officer	Approved by TME 03/08/2023
3.3d	June 2023	Dr Chris Bunch Data Protection Officer	Minor updates and corrections.
3.2	September 2019	Dr Chris Bunch Caldicott Guardian	Minor updates (not ratified)
3.1	February 2018	Dr Chris Bunch Caldicott Guardian	Updated for Data Protection Act 2018. Additional coverage of disclosures
3.0	September 2015	Dr Chris Bunch Caldicott Guardian	Updated as a component policy document of the Information Governance Policy
2.2	February 2012	Dr Chris Bunch Caldicott Guardian	Adapted to new Trust Policy Format / IGG review
1.7	November 2002	Dr Chris Bunch Caldicott Guardian	Approved by Trust Board

Freedom of Information and Environmental Information Regulations Policy

Introduction

1. The Freedom of Information (FOI) Act 2000 is the primary legislation dealing with information rights. It has a strong interface with the Data Protection Act and all other legislation which prohibits or limits the disclosure of information. It provides members of the public with a general right of access to information held by public authorities, supporting openness and transparency across the public sector, and promoting a greater understanding of how public money is spent, and how decisions are taken which affect the services provided by public bodies.

2. The FOI Act imposes a statutory time limit within which requests must be dealt with (20 working days); costs for retrieving and collating information requiring more than 18 hours of staff time may be levied. Responding to freedom of information (FOI) requests depends heavily on access to records to retrieve the information requested or to confirm that it is no longer held. This in turn relies on strict adherence to record management policies and the NHS Records Management Code of Practice.

3. The Environmental Information Regulations 2004 (EIR) provide public access to environmental information held by public authorities in England, Wales and Northern Ireland. Request are handled in the same way as FOI requests, with some minor differences regarding exemptions.

4. The Freedom of Information Act and the Environmental Information Regulations do not give people access to their own personal data (information about themselves), such as their health records. Individuals have a right of access to information held about them under the UK General Data Protection Regulation and the Data Protection Act 2018. This is covered separately by the subject access policy.[1]

5. This document is a component of the OUH Information Governance Policy and should be read in conjunction with the parent policy and its components.

Policy

6. All FOI or EIR requests received must be referred without delay to the freedom of information team (foia@ouh.nhs.uk).

7. The FOI team will follow ICO guidelines and other requirements of this policy and will request and collate information from other staff members as necessary. Staff must respond to all such requests without delay: any concerns regarding admissibility or exclusion of information must be discussed with the Head of Information Governance.

[1] A separate component of the Information Governance Policy.

8. Responses to FOI and EIR requests must be approved without delay by the relevant Divisional Director of Operations (who has delegated Senior Information Risk Owner responsibilities) or an Executive Director before submission to the applicant.

9. Responses must be returned to applicants within 20 working days of receipt by OUH.

10. OUH will operate a publication scheme, providing online access to information regarding its activities which might otherwise result in FOI requests. This is a requirement of Section 19 of the Freedom of Information Act.

11. Information that is exempt from the FOI Act or the EIR or is protected by law will not be released, but the applicant must be informed accordingly within the statutory time frame.

12. Requests for information that is archived, out of date, or inaccessible may also be declined.

Requests for information

13. Requests must be made in writing, on paper or digitally, providing the applicant's full name and contact details. Requests that are not clear and legible may be rejected.

14. As the applicant's identity is only needed to validate the request it must not be used for any other purpose and should not be disclosed when requesting information from staff in other departments.

15. Subject to certain conditions and exemptions (below), applicants may request information which is not included in the OUH publication scheme.

16. Applicants who are not satisfied with the response may appeal by requesting an internal review of the decision, or directly to the Information Commissioner's Office.

Personal and confidential information

17. The release of personal information is primarily governed by the Data Protection Act (2018) and the common law duty of confidentiality. In general, disclosure of personal information requires the individual's consent, unless there is another valid legal basis such as statutory requirement, court order, or an overriding public interest. The Caldicott Guardian is available to advise on such matters if required.

18. Information that identifies individual staff members will not generally be released unless the identity of the individual concerned is already in the public domain, e.g., an executive director. In all cases, the individual must be notified before disclosure.

Document History

Version	Date	Author(s)	Comment
8.3	August 2023	Dr C Bunch, Data Protection Officer	Approved by TME 03/08/2023
8.3d	May 2023	Dr C Bunch, Data Protection Officer	Minor updates
8.2d	September 2021	Dr C Bunch, Caldicott Guardian	Minor updates
8.1	February 2018	Dr C Bunch, Caldicott Guardian	Updated for Data Protection Act 2018
8.0	November 2016	Valerie Gray, Freedom of Information Officer	Updated as component of the Information Governance Policy.

Subject Access Requests

Introduction

1. Organisations which collect and use personal data are required by data protection legislation to provide the individuals concerned (the 'data subjects') details of the information held about them upon request. Such requests are known as 'subject access requests' (SARs).
2. Individuals are entitled to know if any information about them is being processed by Oxford University Hospitals NHS Foundation Trust (OUH), to be provided with a description of the data held, and to be given a copy thereof. They may request specific information, or all information held. They are also entitled to know *why* the information is being held. They are not required to explain why they have requested the information, although this may help to retrieve the relevant information.
3. This document describes how OUH and its staff will discharge this responsibility.
4. This is a component of the Information Governance Policy and should be read in conjunction with that policy and its other components.

Scope

5. These procedures apply to requests received by OUH and its staff from any data subject about whom data is held, including patients, staff and others.
6. This entitlement only applies to living individuals. However, the Access to Health Care Records Act 1990 allows access to information relating to deceased individuals to the personal representative of the deceased, the executor of their will or anyone who has a claim on the deceased's estate. The Access to Medical Reports Act 1988 gives patients the right to see medical reports written about them, for employment or insurance purposes, by a doctor who they usually see in a 'normal' doctor/patient capacity.
7. All members of staff, agency or contracted staff, private sector staff, volunteers and students are expected to follow to the procedures below as well as NHS England's guidance on subject access requests.

Procedures

Making a request

8. Requests from patients for their medical records should be made to the Subject Access Team at the Stable Block, The John Radcliffe Hospital, Oxford OX3 9DU using forms downloadable from the OUH website.
9. Requests from patients for copies of their radiological images should be emailed to pateintimagerequest@ouh.nhs.uk or by post to IM&T's PACS/RIS team, Manor House Annexe, The John Radcliffe Hospital, Oxford OX3 9DU using forms downloadable from the OUH website.

10. Other requests should be sent to the Information Governance Team at Academic Corridor Level 3, The John Radcliffe Hospital, Oxford OX3 9DU using the appropriate form downloadable from the OUH website.
11. There is no charge to the data subject for responding to a subject access request, though a 'reasonable fee' may be charged for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data.
12. Although technically a subject access request, a request by a patient to view their record in a clinical (inpatient or outpatient) setting does not have to be made in writing, provided that the medical team responsible for the patient's care agrees and a member of clinical staff with relevant expertise and/or knowledge can be present to interpret the record as necessary.
13. The OUH legal services department is responsible for processing subject access requests relating to patients and for legal proceedings. The information governance team handle all other requests, including those relating to members of staff and their employment.
14. Data subjects may be required to provide proof of identity and address, normally in the form of passport or driving license, utility bill, bank statement, other document from an official body, or authenticated copies thereof. Staff processing applications are expected to be flexible in their approach to verifying identification and addresses of applicants whilst ensuring that verification is robust.
15. Types of information that may be requested include:
    - health records, letters and notes, on paper or digital;
    - emails;
    - radiological images;
    - photographs, audio and/or video recordings;
    - statements regarding the data subject;
    - information regarding who has accessed their record.
16. A subject access request can be submitted on a data subject's behalf, for example by a relative, guardian, solicitor, other legal professional or an insurance company. The application will require the written consent of the data subject and confirmation of identity. The request must be made and processed in the same way it would if it came directly from the data subject.
17. Where a data subject makes a request for information about them citing the Freedom of Information Act it will be handled as a *subject access request* under the Data Protection Act and the requestor informed accordingly.
18. Requesters may choose to inspect their records rather than applying for a copy of them where the information is not exclusively electronic or there is no intention to process them electronically. This applies where the health record has been modified within the 40 days preceding the request.
19. Children are data subjects in their own right and may make subject access requests if they are mature enough to understand their rights. If not, the request should be made to

their parent or guardian. If in doubt, consult the Caldicott Guardian or the information governance team.

20. **Exemptions.** In some instances, it may not be appropriate to disclose all of the information requested, for example where disclosure:
    - would be likely to cause serious harm to the physical, mental health or condition of the data subject or any other persons;
    - might impair the prevention or detection of serious crime, national security, legal advice or litigation.
21. For a full list of exemptions, consult the Information Commissioner's Office's Subject access guidance or contact the Caldicott Guardian or the information governance team.

Responding to requests

22. Requests should be acknowledged as soon as possible after receipt. A full response must be sent within one calendar month, but the time to respond may be extended by a further two months if the request is complex or a number of requests from the individual have been received, e.g. other types of requests relating to individuals' rights.
23. Responses to subject access requests must:
    - state whether or not OUH holds any personal information about the person concerned;
    - a copy of the information requested;
    - details of the source, if known;
    - a description of the information that is held; the reason for it being processed and whether it has been passed to any other organization or person.
24. The following points should be considered when compiling a response:
    - check with any individual who is identified in the record that they are content for information referring to them being disclosed. If not, consult with the Caldicott Guardian or Senior Information Risk Owner (SIRO) before disclosure and document the decisions made;
    - check whether disclosure would be likely to result in serious physical or mental harm to the data subject or any other person by obtaining permission from the patient's consultant(s) for the release of their medical record. For non- health records consult the Caldicott Guardian or SIRO;
    - agree the method of delivery with the applicant, for example by meeting the individual, by email, or by post (recorded delivery). Reasonable accommodation must be made if the applicant has a disability, for example providing the information in braille, large print or translated into another language.
25. When responding, the applicant should be advised that if they consider any of the information disclosed to be inaccurate this must be reported to the Trust immediately. A patient record may be updated to include the patient's version of disputed information on the approval of the relevant consultant or the Medical Director. This will be recorded in record and the applicant will be informed of any update or the reasons for refusal.

26. If the matter remains in dispute, this should be managed by the OUH complaints procedures. The applicant may also raise the matter with the Information Commissioner's Office.

Document history

Version	Date	Author(s)	Comment
1.5	August 2023	Dr C Bunch Data Protection Officer	Approved by TME 03/08/2023
1.5d	May 2023	Dr C Bunch Data Protection Officer	Minor updates
1.4d	September 2019	Dr C Bunch, Caldicott Guardian	Minor updates
1.3	February 2018	Dr C Bunch, Caldicott Guardian	Updated as a procedural document and for the Data Protection Act 2018
1.2	May 2017	Nuala Buchan Brodie, IG Manager	Updated as a component policy document of the Information Governance Policy
1.1	January 2017	Nuala Buchan Brodie, IG Manager	New policy

NHS Number Policy

Introduction

1. The NHS Number is a unique ten-digit number used to identify individual patients and match them to their health records. Everyone registered with the NHS in England, Wales and the Isle of Man has their own unique number.

2. NHS Numbers are issued and maintained as part of the NHS Personal Demographics Service (PDS), also known as the 'Spine'. The normal method of accessing the PDS is via the electronic patient record (EPR).

3. A key purpose of the NHS number is to improve patient safety by reliably linking patients to their records. The NHS Number should be present in all active patient records, both paper and IM&T.

4. This document is part of the Oxford University Hospitals NHS Foundation Trust (OUH) Information Governance Policy and should be read in conjunction with that policy and its other components.

Policy

5. Each patient's NHS Number must be and determined, recorded and used as early as possible in every episode of care.

6. At first contact, the patient's NHS Number must be recorded on the Electronic Patient Record (EPR), where it will be automatically available for subsequent encounters.

7. When a patient's NHS Number cannot be ascertained, the medical record number (MRN) should be used until the NHS Number is available.

8. The NHS Number (or MRN if not available) must be recorded on every single page of their paper record (if it exists), using adhesive labels and following positive patient identification. Where labels are unavailable, it should be written in the '3 3 4' digits format to reduce the likelihood of transcription errors or when reading the numbers.

9. Whenever possible, standard letter or documentation templates should include the NHS Number automatically, removing the need to enter the NHS number manually.

Scope

10. This policy applies to all staff in all areas of OUH, including those employed by a third party or external contractors, voluntary workers, students, locums and agency staff.

Responsibilities

11. **Clinical, secretarial and clerical staff** must ensure that the NHS Number is quoted in all patient-related communications and documents, preferably using an adhesive ('sticky') ID label.

12. **Staff receiving external patient referrals** must check that the referral has the patient's correct NHS Number, and that this is registered on the EPR together with all necessary demographic data. Any problems must be logged via the OUH Information Management & Technology (IM&T) service desk imandtservicedesk@ouh.nhs.uk.

13. **Clinical computer system managers** must ensure that their systems obtain patient demographic data in real time directly from central OUH systems, as directed by IM&T Services.

14. **IM&T staff responsible for data quality** must:

    - ensure that missing NHS Numbers are sourced and registered on the EPR within 24 hours for inpatients or in good time before an elective admission or procedure;
    - ensure that where NHS Numbers are not available, a special MRN is issued as a temporary NHS number;
    - resolve IM&T service desk calls regarding NHS Numbers within four hours if possible;
    - escalate data quality problems to the National Back Office via the IM&T service desk immediately upon identification;
    - run reports of patients without NHS Numbers to check if one has since been issued.

Untraceable NHS Numbers

15. There will be occasions when an individual's NHS Number cannot be traced. This may be because they have never been registered electronically with any GP. In these circumstances, the clinical team should contact the patient's GP practice to confirm that the patient is registered there. If recently registered there may be an internal delay in the information appearing on EPR.

Document history

Version	Date	Author(s)	Comment
1.2	August 2023	Dr C Bunch Data Protection Officer	Approved by TME 03/08/2023
1.2d	May 2023	Dr C Bunch Data Protection Officer	Minor updates
1.1	September 2021	Dr C Bunch, Caldicott Guardian and Data Protection Officer	Minor updates
1.0	February 2018	Dr C Bunch, Caldicott Guardian	Adapted from earlier versions as a component of the Information Governance Policy and to comply with the Data Protection Act 2018

Data Quality Policy

Introduction

1. Modern healthcare relies heavily on information for clinical care, administration, management, finance, research, planning, and external reporting. The data required to support these activities is complex and its quality is of the utmost importance.
2. This document describes the key pillars of data quality, its scope and the standards that Oxford University Hospitals NHS Foundation Trust (OUH) expects to assure its activities are supported by the highest quality data.
3. NHS organisations, including OUH, are required to make submit regular and ad hoc data submissions centrally. The quality of these is monitored by NHS Digital through a Data Quality Maturity Index. Organisations are also required to evidence their data quality performance annually through the NHS Digital Data Security and Protection Toolkit (DSPT)[1].
4. This document is a component of the OUH Information Governance Policy and should be read in conjunction with the parent policy and its other components, in particular the Information Governance Framework.

Scope

5. This policy applies to all data collected and created to support OUH clinical and non-clinical activities, whether on paper or held digitally on any system. This includes *metadata*—data that provides data about other data[2]. Relevant metadata supports data quality work and helps users to assess whether the data set is adequate for their use.
6. It applies to all staff working across OUH, in whatever capacity, including agency, bank and volunteers, or sub-contractors. It applies also to staff employed elsewhere who are working on a research project within OUH.

Policy

7. All staff must be aware of and work to the standards set out in this policy, and strive to ensure that all data collected and recorded for any purpose is of the highest possible quality.
8. Clinical staff must ensure that clinical information is recorded in line with this policy and the *Clinical standards for documentation and record keeping* section of the Health Records Management Policy.

[1] A comprehensive description of expected compliance with data quality requirements of the DSPT is given in pp. 35–47 of the DSPT Data security standards - big picture guide 01: Personal confidential data.
[2] Wikipedia: https://en.wikipedia.org/wiki/Metadata. Accessed 4th May, 2023.

9. Non-clinical staff must ensure that information is recorded in line with this policy and the NHS Records Management Code of Practice (2021).

10. External data reporting must comply with this policy and with the NHS Information Standards.

The pillars of good data quality

11. There are several key characteristics of good quality data, for example:

Accuracy

12. All data must be accurate and kept up to date. For example, all reference tables, including GPs and postcodes must be updated regularly and usually within a month of publication. Patients' demographic details must be checked with the patient themselves at every inpatient, outpatient and any other service contact, following specific standard operating procedures (SOPs) as inaccurate demographics may result in important letters being mislaid, or the incorrect identification of patients.

Validity

13. Data must be collected and maintained in formats that conform to national or local standards, for example the NHS Data Model and Dictionary, the NHS Records Management Code of Practice, and NHS Digital's Information Standards. Codes must map to national values and wherever possible, computer systems should be programmed to only accept valid entries.

Reliability

14. Data must reflect stable and consistent data collection processes across collection points and over time, whether using paper or digital systems, or a combination. Stakeholders should be confident that progress toward performance targets reflects real changes rather than variations in data collection approaches or methods.

Timeliness

15. Data must be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable period. Data must be available quickly and updated often enough to support information needs, mandatory deadlines, and to support the right clinical or management decisions.

Relevance

16. Data captured should be relevant to the purposes for which it is used. This entails periodic reviews of requirements to reflect changing needs.

Completeness

17. Data requirements should be clearly specified based on clinical, non-clinical and external information needs of the organisation, with data collection processes designed to fulfil these requirements. Monitoring missing, incomplete, or invalid

records can provide an indication of data quality and can also point to problems in the recording of certain data items.

18. All mandatory data items within a data set should be completed and default codes only used where appropriate, not as a substitute for real data. For key data items which are not mandatory, it is important to produce a list of records with missing items to be actioned later.

19. Monitoring missing, incomplete, or invalid records can provide an indication of data quality and can also point to problems in the recording of certain data items.

Responsibilities

20. **All staff.** The fundamental principle of data quality is that data should be right first time, which means that the responsibility lies with the person recording the information at the point at which it is collected, whether is clinical, or non-clinical. Therefore, all staff are responsible and accountable for the quality of data they collate and record. Staff must ensure that they comply with the requirements of this and other policies and procedures relating to their role.

21. Specific responsibilities for implementing the Information Governance Policy, of which this is a component, are given in the parent policy document.

22. The **Director of Data and Analytics** has overall responsibility for data quality and ensuring the operational delivery of this policy and any associated processes or procedures.

23. The **Head of Data Quality**[3] has day-to-day responsibility for implementing this policy, and monitoring compliance.

Auditing data quality

24. The Head of Data Quality will coordinate and oversee an annual data quality audit programme including audits undertaken by OUH staff, and audits to be undertaken by OUH's internal auditors—normally biennially.

25. Scoping of the data quality audits will be undertaken by Head of Data Quality, who will identify the services to be audited and the requirements for validation. All audits will result in a finding and recommendations report including, where appropriate, an action plan, and reported to the Digital Oversight Committee.

Monitoring compliance and effectiveness

26. The collecting and processing of data will be regularly monitored to ensure compliance with the standards in this policy as well as national standards, and to provide feedback to staff. This will be coordinated by the Head of Data Quality and reported through the Digital Oversight Committee.

[3] Presently under discussion. The post has not been filled since previous occupant retired in 2019.

27. Regular reports on performance indicators will be provided to operational managers to review and to support the development of targeted improvement plans and divisional performance reviews.

28. Where outcomes are found to be unsatisfactory, the underlying cause(s) will be determined and measures instituted at divisional, team or individual level to restore data quality to the required standard.

Document History

Version	Date	Author(s)	Comment
5.1	August 2023	Chris Bunch, Data Protection Officer Mark Currie, Director of Data and Analytics	Approved by TME 03/08/2023
5.1d	June 2023	Chris Bunch, Data Protection Officer Mark Currie, Director of Data and Analytics	Minor updates.
5.0d	August 2021	Steve Chokr, Dr Chris Bunch Caldicott Guardian	Rewritten as component policy of the Information Governance Policy and to incorporate internal audit recommendations. (Not ratified)