Information Governance Policy

Category:	Policy
Summary:	Updated for Data Protection Act 21018 compliance
Equality analysis undertaken:	November 2016
Valid from:	
Date of next review:	January 2021
Approval Date/ via:	21st February 2018 via Information Governance and Data Quality Group
Distribution:	Trust-wide
Related documents:	See main document for list of component documents
Authors:	Nuala Buchan-Brodie, Information Governance Manager Dr C Bunch, Caldicott Guardian
Further information:	Information Governance
This document updates:	Information Governance Policy v9.1

Lead Director: Chief Information and Digital Officer
Issue Date:

Contents

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, 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. Relevant legislation includes the Data Protection Act (2018, incorporating the EU General Data Protection Regulation), Freedom of Information Act (2000), Human Rights Act (1998), Access to Health Records Act 1990 and the Care Act 2014. Other relevant guidance is included below.

5. The Trust 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.

6. This is one of three over-arching policies covering information governance. The other two are the Information Protection Policy and the Records Policy.

Policy statement

7. It is the policy of the Trust that all employees and parties must maintain the highest standards in all matters concerning the use, handling, protection, transmission and sharing of information held by the Trust, and must at all times act lawfully and take note of the guidance set out in this policy and its accompanying documents.

8. This policy comprises this document and the following component policy documents:
    - Information governance framework;
    - Confidentiality and disclosure
    - Freedom of information and environmental information;
    - Subject access requests;
    - NHS number.

Scope

9. 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

10. The purpose of this policy is to ensure high standards of information governance throughout the Trust.

Definitions

11. 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.

Responsibilities

12. The *Chief Executive,* as the Accountable Officer, has overall responsibility for information governance and is required to provide assurance through the Statement of Internal Control that all risks to the Trust are effectively managed and mitigated.

13. 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.

14. The *Caldicott Guardian* is responsible for overseeing and advising on processes to satisfy the highest standards for handling personal identifiable information.

15. The *Data Protection Officer* independently advises on and monitors the Trust's data processing activities and data security.

16. The *Information Governance Manager* is responsible for supporting and monitoring the implementation of this policy.

17. *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.

18. 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

19. Training required to fulfil this policy will be provided in accordance with the Trust's training needs analysis. Management and monitoring of training will be in accordance 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

20. 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 training and information - related incidents	Information Governance Manager. Divisional General Managers.	Monthly	Information Governance and Data Quality Group Data Protection Officer
Policy implementation and staff compliance	Spot checks of departmental areas and audits	Information Governance Officer	Ongoing	Information Governance and Data Quality Group Data Protection Officer

Review

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

22. Component policy documents, as listed in paragraph 6, 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.

References

23. National guidance and reference documents:

- NHS Digital: Data Security and Information Governance
  NHS Digital offers guidance on looking after information well according to the principles of good information governance (IG).
- The Information Governance Alliance
  The IGA is the authoritative source of advice and guidance about the rules on using information in health and care.
- To Share or Not to Share. The Information Governance Review
  Informally known as Caldicott2, this considers how information about patients is shared across the health and care system. It introduced a new Caldicott principle — Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality. It also sets out actions required by Caldicott Guardians in health and social care.
- Caldicott2 Implementation Home Page
  The information on these pages is intended to assist organisations to implement the recommendations of relevance to them contained in the Caldicott2 Report. It provides information on topics such as monitoring and networks
- The National Data Guardian's Review of Data Security, Consent and Opt Outs
  Published in July 2016, this is the latest report from Dame Fiona Caldicott in her role as the National Data Guardian. The review provides 20 recommendations and 10 data security standards aimed at strengthening the security of health and care information, and ensure people can make informed choices about how their data is used.
- Data security review: letter to NHS Trusts
  Just prior to the publication of the review of data security, consent and opt-outs, Dame Fiona Caldicott, the National Data Guardian (NDG), and David Behan, Chief Executive of the CQC, wrote a joint letter to NHS trusts. The letter outlines what trusts should be doing now in the area of data security. This is a succinct aide memoire to check compliance within your organisation, especially if you are subject to CQC audits.
- CQC report *Safe data, safe care*
  Covers how data should be safely and securely managed in the NHS. Makes recommendations *inter alia* on training for Caldicott Guardians and SIROs.
- Information Governance Toolkit (IG toolkit)
  The IG Toolkit is an online system which allows organisations to assess themselves or be assessed against Information Governance policies and standards. It also makes available participating organisations' IG performance

available to members of the public. It will be replaced by the Data Protection and Security Toolkit from April 2018.

- Information sharing: the Information Commissioner's Office code of practice
- Records Management: NHS Code of Practice for Health and Social Care 2016
  Sets out standards required for the management of NHS records — both paper and digital. When sharing data, organisations need to ensure their own records management policies align with those with whom and whose data is shared. For example if your local polices allow for data to be held for three years but another organisation holds it for two years, you could, by default become the data controller for their originating information.
- ICO guidance on data protection reform: the GDPR and Data Protection Bill.

Equality analysis

24. 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 Annex). As this policy applies to all staff equally, no detriment was identified to any group and no adjustments are required.

Document History

Date of revision	Version number	Reason for review or update
Oct 2006	v1	IG Toolkit requirement
Dec 2007	v2	Routine update
Nov 2008	v3	Routine update
Dec 2009	v4	Routine update
Mar 2001	v5	Routine update
Mar 2012	v6	Routine update
Mar 2012	v7	Routine update
Jan 2014	v8	Routine update
Apr 2014	v9	Updated and converted to IG policies format
Nov 2016	v9.1	Minor corrections
Nov 2017	v9.2	Minor updates for consistency with the GDPR

Annex: Equality assessment

Equality assessment: Information Governance Policy
November 2016
Review date: *November 2020*
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 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 Information Governance and Data Quality Group. 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.*
How does the policy advance equality of opportunity? *n/a*
How does the policy promote good relations between groups? *n/a*

The Information Governance Framework

Introduction

1. This framework sets out the arrangements for the management and implementation of information governance throughout the Trust.

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

Scope

3. This framework covers all areas of the Trust and all who work therein and handle information, whether or not Trust employees.

4. Information governance comprises the following key areas:

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

Governance, compliance and assurance

People

5. The *Senior Information Risk Owner (SIRO)* has delegated responsibility and authority for information governance and implementation of relevant policies. The present SIRO is Sara Randall.

6. The *Caldicott Guardian* oversees and advises on the confidentiality and handling of personal identifiable information. The present Caldicott Guardian is Dr Chris Bunch.

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

8. The *Information Governance Manager* is responsible for supporting and monitoring the implementation of this policy, and is accountable to the SIRO. The present Information Governance Manager is Nuala Buchan-Brodie.

9. The *Information Governance* and *Freedom of Information (FOI) Officers* support and are accountable to the Information Governance Manager, with general responsibility for information governance matters and freedom of information. The present Information Governance and Freedom of Information Officers are Robin Peach-Toon, Alex Chan and Jenny Kitovitz.

10. The *Head of IM&T Services* is accountable to the SIRO for the provision, management and governance of the Trust's major information technology (IT) systems. The present Head of IM&T is John Skinner.

11. The *Data Quality Manager* is accountable to the SIRO for all aspects of data quality and audits. The present Data Quality Manager is Francine Tanner.

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

13. Each Division has an information governance lead who provides liaison between their Division and the IG team, and who attends meetings of the Information Governance and Data Quality Group (see below.) IG leads are expected to take ownership of, and seek to improve, the quality of information and its management within their service.

14. Together, the Information Governance Manager, Information Governance Officer and the Freedom of Information Officer comprise the Information Governance Team, which can be reached at information.governance@ouh.nhs.uk.

15. The Trust will appoint a Data Protection Officer in accordance with the requirements of the Data Protection Act (2018). The DPO will provide independent advice and assurance on all matters relating to data protection.

The Information Governance and Data Quality Group (IGDQG)

16. The Information Governance and Data Quality Group (IGDQG) is the primary body overseeing and supporting information governance within the Trust, 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.

17. Its purpose is to support and drive the data quality and information governance within the Trust, ensuring the Trust 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.

18. IGDQG meets bi-monthly and reviews progress with the information governance toolkit (IGTK), policies, procedures & guidance, incident reports, information governance and data quality audits.

19. IGDQG is co-chaired by the Caldicott Guardian and the SIRO, and reports to the Trust Audit Committee.

20. Membership[1] includes the Caldicott Guardian and Senior Information Risk Owner (co-chairs), the information governance team, Chief Clinical Information Office,

[1] The full membership list and terms of reference are available on the information governance intranet pages.

representatives from IM&T, finance, human resources, training, health records, clinical coding and Divisional information governance leads.

Information assets

21. 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. Key information assets, including all assets which include person-identifiable information, must each have a information asset owner and, optionally, an administrator.

22. *Information asset owners (IAOs)* are responsible for documenting and registering information assets and information transfers and ensuring their security. IAOs must have undergone suitable training for their role before assuming responsibility, and will be accountable in this role to their divisional general manager.

23. *Information asset administrators (IAAs)* may be assigned day to day responsibility for each information asset to support the IAO.

24. *Divisional general managers* have devolved SIRO responsibilities for information assets within their division.

25. All information assets and transfers that concern person-identifiable information will be recorded on a central register. 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, and an assessment of the risks posed to the Trust.

26. The IAO is responsible for identifying, documenting and registering information assets and data transfers within their respective team or department.

The information governance toolkit (IGTK)

27. Each year, NHS organisations must report centrally on their implementation of standards set out in the national information governance toolkit. The IGTK covers a comprehensive set of information governance standards and provides evidence of their implementation, measures compliance against the law and national guidance, and demonstrates whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

28. From April 2018 an extensively revised toolkit (the Data Security and Protection Toolkit) with greater emphasis on information security will replace the existing IGTK.

Information governance statement of compliance

29. All organisations who wish to use NHS Digital's systems and services, including the NHS network, must sign an agreement that sets out terms and conditions for use and includes a range of security related requirements which must be satisfied to assure the integrity of the NHS network and information assets that may be accessed.

30. The IG assurance statement is a required element of the IGTK and is re-affirmed at the time of annual self-assessment submission. This statement is approved and signed by the SIRO.

Information-related incidents and reporting

31. All staff are expected to report, via the Trust incident reporting system Datix, any actual or potential incidents involving information. 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.

32. Serious incidents will be categorized in accordance with the Department of Health's checklist.

33. IGDQG will monitor and review serious untoward incidents and events, ensure remedial and preventative measures are/have been taken. The SIRO and Caldicott Guardian will be informed immediately of all serious incidents involving the unauthorised disclosure of person-identifiable information.

Audit

34. The Trust will undertake or commission annual assessments and/or audits of:

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

Privacy notices

35. The Trust will a publish privacy notice informing patients of how it will use the information it collects about them, in accordance with the Data Protection Act 2018. This must clearly signposted on every page of any website that carries the OUH brand , and will also be available through the Trust's internet web pages, information leaflets, and posters displayed at patient reception points.

36. The Trust will also provide staff with a privacy notice detailing how the Trust uses information it collects about individual staff members.

Data protection impact assessments

37. The Trust requires a 'privacy-by-design- approach to all systems and processes that involve person-identifiable data. A data protection impact assessment 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, service, system or process.

38. The information governance team must be consulted during the conception and design phase of any new information asset, service, system or process, *before* procurement. The team will advise on and approve completed assessments.

External contractors

39. 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.

40. The procurement department is responsible for the monitoring and review of contracts for external contractors to ensure that information governance 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.

41. 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.

42. 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.

43. The NHS standard contract template covers the most important information governance aspects, but it 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

44. The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

45. 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 Trust.

46. IM&T Services has responsibility for cyber security, supported by a cyber security analyst and task force.

Confidentiality, information sharing and disclosure

47. The Trust is custodian 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.

48. The Caldicott Guardian is responsible for advising the Trust and its staff on matters relating to confidentiality, information sharing and disclosures.

Freedom of information and subject access requests

49. The Freedom of Information Act 2000 (FOAI) 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.

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

51. 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.

52. Subject access requests are covered by the Subject Access Request Policy component of this policy.

53. Requests related to medical records are handled by Legal Services. Requests for radiology images are handled by IM&T Services.

Quality assurance

54. 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.

55. The Trust will ensure that as far as possible the quality of its information can be assured from its point of collection or acquisition, and through any subsequent use.

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

57. The Trust Data Quality Policy provides the framework for information quality assurance.

Training

58. All Trust staff must undertake annual basic information governance training. Staff handling patient information must also undertake additional training at a level commensurate with their role. Face-to-face training sessions will be arranged for staff who do not have access to online training.

59. 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 Trust's Learning and Development Policy. This information can be accessed via the Learning and Development pages on the Trust intranet.

Document history

Date of revision	Version number	Author(s)	Reason for review or update
Mar 2018	v3.3	Chris Bunch	Minor corrections
Jan 2018	v3.2	Chris Bunch	Updated for GDPR
Mar 2017	v3.1	Chris Bunch	Updated IAO section
Nov 2016	v3.0	Nuala Buchan Brodie and Chris Bunch	Rewritten for 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 *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 patient confidentiality. It applies equally to information regarding other individuals, including staff.
5. Alongside the duty of confidence 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 Trust's 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 confidence.
[2] Principally the Data Protection Act (2018) which incorporates the EU General Data Protection Regulation.

Awareness and compliance

10. Everyone in the Trust 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 Trust's 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 Trust's 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 confidence

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 will be able to register their wish to opt out of the use of their information for secondary uses from May 25th 2018 via a national NHS scheme. Providers will have to respect any opt outs no later than 2020.

19. The duty of confidence is not absolute: in some circumstances, such as individual (direct patient) care, the 'duty to share' can be as 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 the 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	The Chief Environmental Health Officer of the relevant local authority, through the consultant in communicable Disease Control on Environmental Health and Protection Notification Certificates
Poisonings and serious accidents at the workplace	Doctor currently responsible for patient's welfare	To the Health and safety Executive via the Personnel Department of on-call manager using form UCH291. The information should be reported as soon as possible and does not have to wait till the next working day.
Abortions	The doctor who terminates the pregnancy	To CMO (DSS) on form HSA4
Drug addicts	The doctor in attendance	CMO (Home Office) on form FO9 – Notification of Drug Addiction
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

- A Court of Law (including Coroners Court and Industrial Tribunals)
- Health Service Commissioner
- Health and Safety Commission
- Health and Safety Executive
- Inquiries appointed by the Secretary of State
- Employment Medical Advisers
- Professional bodies of the Health Professions – doctors, dentists, nurses, midwives, health visitors, opticians and professions allied to medicine (but not pharmacists)
- Mental Health Act Commission
- Mental Health review 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: 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

Trust policies and guidance

- Information Sharing Policy
- Information Protection Policy

External guidance

- Confidentiality. NHS Code of Practice (2003)
- HSCIC Guide to Confidentiality
- HSCIC Confidentiality Code of Practice
- 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
- Improving information sharing between Police and health services

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
3.1	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 Protection 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 Act 2000 (FOAI) 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 FOIA imposes a statutory time limit within which requests must be dealt with (20 working days), and there is an upper limit charges for disproportionate costs for retrieving and collating information. 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 the Trust's record management policies and the NHS code of practice for records management.

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 Data Protection Act 2018. This is covered by the Trust's subject access policy.[1]

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

Policy

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

7. The team will request 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 IG manager.

8. Responses to FOI and EIR requests must be approved by the Senior Information Risk Owner before submission to the applicant.

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

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

10. The Trust will operate a publication scheme, providing online access to information regarding the Trust and 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 FOIA 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. Subject to certain conditions and exemptions (below), applicants may request information which is not included in the Trust's publication scheme.

14. 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.

15. 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

16. The release of personal information is primarily governed by the Data Protection Act (2018) and the common law duty of confidence. 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 as required.

17. 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
8.1	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'.
2. Individuals are entitled to know if any information about them is being processed by the Trust, to be provided with a description of the data held, and to be given a copy thereof. 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 the Trust 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 the Trust and its staff form any data subject for 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 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.
7. All members of staff, agency or contracted staff, private sector staff, volunteers and students are obliged to follow to the procedures below. Further information is available in the Information Commissioner's Office's Subject access code of practice.

Procedures

Making a request

8. Details of how to make a subject access request are available on the Trust's website. In brief requests from patients should be made to the Subject Access Manager at the Data Quality Department, West Wing Level 3, The John Radcliffe Hospital, Oxford OX3 9DU using forms downloadable from the website.
9. 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 website.
10. Until 25th May 2018 the Trust may charge for each request for information held digitally For medical records the charge is up to £50, for all other records £10.
11. 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

staff with relevant expertise and/or knowledge can be present to interpret the record as necessary.

12. The Trust's legal services department is responsible for processing subject access requests relating to patients and legal proceedings, though most routine patient requests will be managed by medical records staff. The information governance team handle all other requests, including those relating to members of staff and their employment.

13. 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

14. 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;
    - references and/or statements regarding the data subject.

15. 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 proof of identity. The request must be made and processed in the same way it would if it came directly from the data subject.

16. Where a solicitor, other legal professional or insurance company request access on behalf of a data subject, access may be given with the consent of the Data Subject. The legal professional must have written and signed consent 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. Requestors 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 some or 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 code of practice or contact the Caldicott Guardian or the information governance team.

Responding to requests

22. Responses to subject access requests must:

    - state whether or not the Trust holds any personal information about the person concerned
    - a description of the information that is held; reason for it being processed and whether it has been passed to any other organization or person;
    - a copy of the information requested;
    - details of the source, if known.

23. 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 whether 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.

24. 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 willl be recorded in record and the applicant will be informed of any update or the reasons for refusal.

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

Document history

Version	Date	Author(s)	Comment
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 number.

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

4. This document is part of the 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 with the Trust, patients' NHS Number must be determined and recorded on the EPR, where it will be automatically available for subsequent encounters.

7. When a patient's NHS Number cannot be ascertained, the Trust medical record number 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, preferably using adhesive labels and following positive identification. Where labels are unavailable it should be written in the '3 3 4' format to reduce the likelihood of transcription errors or when reading the numbers.

9. Whenever possible, standard letters or documentation 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 the Trust, 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 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 IM&T service desk.

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

14. **Data quality staff** 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 helpdesk 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 are some whose NHS Numbers 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
1.0	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