Document Control

Title			
Confidentiality Policy			
Author Acting Information Governance Lead		**Author's job title** Acting Information Governance Lead	
Directorate Finance and Performance – IM&T		**Department** Informatics - Information Governance	
Version	**Date Issued**	**Status**	**Comment / Changes / Approval**
1.0	Jan 2008	Final	Ratified by Trust Board
1.1		Revision	Revised by Caldicott Group
1.2	Feb 2011	Revision	Updated with guidance on removable devices and (2.1 – 2.7 and Appendices A – C) elements from previous Devon PCT Code of Practice. Re-formatted into corporate template and proof-checked in accordance with Policy on Policies. Presented to the Trust Data Protection & Confidentiality Group 7/1/2011 and approved by Information Governance Steering Group 2/2/2011
1.3	May 2011	Revision	Updated with guidance on control of photography and safe use/ disposal of ward handover sheets. Presented to the Trust 27/5/2011 Data Protection & Confidentiality Group.
1.4	Nov 2011	Revision	Additional guidance on mailing Person Identifiable Data (section 9.3). Data Protection & Confidentiality Group (DP&C) 18/11/2011.
1.5	Jan 2012	Revision	Additional guidance on e-mail and password protection recommended by Data Protection & Confidentiality Group.
1.6	Apr 2012	Revision	Additional guidance on staff accessing their own or family information (section 8.1).
1.7	Oct 2012	Revision	Minor amendments by Corporate Governance to update document control report, version control, headers and footers, formatting for document map navigation and table of semi-automatic contents, and updated Equality Impact Assessment.
3.0	Nov 2012	Final	Harmonised policy as a result of the merging of Northern Devon Healthcare NHS Trust and NHS Devon community services. Reviewed by Data Protection & Confidentiality Group on 26th October meeting and forwarded for approval at Information Governance Steering Group on 19th November following consultation. A summary of key issues and differences is on page 3.
3.1	Jun 2014	Revision	Addition of new Caldicott 2 principle to share. Update to main contact.
3.2	May 2015	Draft	Substantial re-write to facilitate a more integrated IG Policy framework and remove duplication where possible
3.2.2	May 2015	Draft	Amended after internal IG discussion and review
3.2.3	Jun 2015	Draft	Completed mapping to Caldicott 2 recommendations
3.2.4	Jun 2015	Draft	Amendments following consultations

4.0	03.08.15	Final	Approved by IG & IM&T Steering Committee
4.1	11.12.15	Final	Corrections approved by Director of F&P
4.2	23 Mar 2018	Revision	Approved by IG & IM&T Steering Committee to support IG Toolkit compliance. Review date extended by one year to allow complete GDPR guidance to be incorporated.

Main Contact Acting Information Governance Lead Information Governance Department 23 Castle Street Barnstaple EX31 1ET	**Tel: Direct Dial** – 01271 341477 **Email**: ndht.informationgovernance@nhs.net

Lead Director
Director of Finance & Performance

Superseded Documents

Issue Date	Review Date	Review Cycle
March 2018	March 2019	One year

Consulted with the following stakeholders:

- Systems Managers and Department Heads across the Trust
- Peer Review – SIGN

Approval and Review Process

- Director of Finance & Performance / IG & IM&T Steering Committee – Approval
- Head of Information Governance - Review

Local Archive Reference
X:\Information Governance
Local Path
\Information Management\Information Governance\Policy Development
Filename
Confidentiality Policy V4.2 Mar18.docx

Policy categories for Trust's internal website (Bob)	Tags for Trust's internal website (Bob)
IM&T Services , Information Governance	Asset, Private, Personal, Confidentiality, Confidential, Data, Security, Information, Governance, Protection, Sensitive, Caldicott, Privacy,

CONTENTS

1. Purpose

1.1. The purpose of this document, and its associated guidance in the Information Governance Handbook, is to ensure adherence to statutory and legal frameworks relating to confidential personal data, including:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- The Law of Confidentiality – See below section 2.4

1.2. The policy sets out Northern Devon Healthcare NHS Trust's approach to the management of confidential information to ensure a consistent approach across the whole organisation. It supports the duties set out in the NHS Constitution. It applies to all Trust staff (including temporary and agency staff and volunteers) – see below at 11 Glossary Appendix A. Staff must comply with this policy as a condition of their employment. A breach of confidentiality may result in disciplinary action.

1.3. Whilst this policy sets out the legal framework and standards which must be applied, more detailed guidance on implementation will be found in the Information Governance Handbook.

1.4. Implementation of the policy, and that guidance, will ensure that staff will:

- Understand everybody's right for their information to be kept confidential
- Respect everybody's right to be consulted on the use of their confidential information
- Recognise what constitutes personal confidential data
- Recognise other information which must be treated as confidential e.g. because it is commercially sensitive or because uncontrolled disclosure may prejudice the proper and effective management of the Trust and its
- Take appropriate measures to protect all confidential information

1.5. This policy applies wherever there is a duty of confidentiality. For convenience it often uses patient information as the legal context but applies equally to all circumstances. It provides a minimum legal standard. Additional ethical standards shall apply where government and professional regulatory bodies require. Staff are expected to be familiar with, and adhere to, such standards where they apply to their work.

1.6. Finally this policy takes into account those recommendations of the Information Governance Review (also known as the second Caldicott report) which apply directly to the work of the Trust. Those recommendations and the steps taken by the Trust are summarised in 12 Appendix B below.

2. Legal Context

Administrative law

2.1. The Trust must act within its lawful powers. The NHS Act 1997 provides the Trust with the power to do anything which appears to it to be necessary or expedient for the purpose of, or in connection with the provision of services for the purposes of improving physical and mental health of the people of those countries, and the prevention, diagnosis and treatment of illness.

2.2. Explicit duties to disclose confidential information are provided in some statutes. For example:

- The Trust must act within its lawful powers. The NHS Act 1997 provides the Trust with the power to do anything which appears to it to be necessary or expedient for the purpose of, or in connection with the provision of services for the purposes of improving physical and mental health of the people of those countries, and the prevention, diagnosis and treatment of illness.
- Explicit duties to disclose confidential information are provided in some statutes. For example:
- Section 8 of the National Audit Act 1983 imposes a legal obligation on public bodies to provide relevant information to the National Audit Office.
- Section 45 of the Care Act 2014 imposes a legal obligation to disclose to a Safeguarding Adults Board if certain conditions are met.
- Section 47 of the Children Act 1989 imposes a legal obligation to supply information to a Local Authority exercising its child protection powers unless it would be unreasonable to do so.
- In very limited circumstances the Trust may be required to disclose confidential information under the Freedom of Information Act 2000 if it was not received from another person or if disclosure would not be actionable by another person. The Freedom of Information Act 2000 provides other exemptions which will typically avoid disclosure in such cases e.g. the exemption for personal data.

2.3. Other statutes provide powers to share information. For example section 115 of the Crime and Disorder Act 1998 provides a power to share information between specific agencies for the purpose of preventing crime and disorder.

Common law duty of confidentiality

2.4. Confidentiality is a common law concept built up from case law where practice has been established by individual judgements of the Courts.

2.5. A duty of confidentiality arises when one person shares information with another (e.g. patient to doctor/ nurse) in circumstances where there is a reasonable expectation of confidentiality based on the nature of the relationship. The duty equally applies to information about the patient created by the Doctor because of that relationship. All patient information is thus held under legal and ethical obligations of confidentiality and should not be used or disclosed in a form that might identify a patient without his or her consent unless there is a need and clear legal basis to do so.

2.6. A duty of confidentiality also arises in other situations e.g.

- Personal information held by the Trust relating to staff may attract a duty of confidentiality because there is a reasonable expectation of confidentiality in the employer / employee relationship. Not all information is covered by this duty. For more information about the extent of the duty please see the Disclosure of Staff Information Policy.
- Information arising out of Trust commercial contracts and related procurement exercises may be subject to a duty of confidentiality.
- Information relating to internal Trust business e.g. relating to management meetings, including Board meetings which are closed to the public, should be regarded as confidential by staff who have access to it and is covered by the confidentiality clause in employment contracts. This applies even though some of this information may be disclosable if requested under the Freedom of Information Act. Such disclosures may only be made in accordance with the Freedom of Information Policy and Procedure.

2.7. The key principle is that confidential information may only be used or disclosed with the consent (which may be implied) of the person to whom the duty of confidentiality is owed unless there is a need and clear legal basis to do so. This need includes the need to share pertinent information to provide good clinical care which must be balanced against the need to protect patient information.

2.8. Unauthorised use or disclosure of confidential information without lawful justification may result in an action for damages against the Trust and disciplinary action against anyone responsible.

Data Protection Act 1998

2.9. This Act has close links with confidentiality as all processing of personal data must be lawful to comply with the data protection principles. Lawfulness includes complying with the duty of confidentiality.

2.10. For more information see Trust's Data Protection Policy.

Human Rights Act 1998

2.11. Article 8 of the Human Rights Act 1998 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records.

2.12. In general compliance with the Data Protection Act 1998 and the common law of confidentiality should satisfy Human Rights requirements.

2.13. The Human Rights Act may occasionally require a wider consideration of the rights of family or relatives in addition to the rights of the person to whom a duty of confidentiality was owed.

NHS Act 2006

2.14. Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes where it is not possible to use anonymised information and where seeking consent is not practical, having regard to the cost and technology available.

2.15. Details of current approvals may be found on the Health Research Authority Website.

3. Definitions

3.1. See also part 11 Appendix A – Glossary of terms and abbreviations and the HSCIC IG Toolkit Glossary of Terms.

Personal data / personal information

3.2. 'Personal data' is defined in the Data Protection Act 1998 as information *relating to a living identifiable individual*. Where the term is used in this policy or the Information Governance Handbook it has this Data Protection Act technical meaning. The term 'personal information' is used in a looser sense to refer to any information about a person.

Sensitive Personal Data

3.3. Sensitive personal data is defined in section 2 of the Data Protection Act 1998 as personal data consisting of information as to:

"(a) the racial or ethnic origin of the data subject

(b) his political opinions

(c) his religious beliefs or other beliefs of a similar nature

(d) whether he is a member of a trade union

(e) his physical or mental health or condition

(f) his sexual life

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."

Personal Confidential Data

3.4. This term describes personal information about identified or identifiable individuals, which should be kept private or secret. 'Personal' includes the Data Protection Act definition of personal data and sensitive personal data (see above), but it is extended to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

Confidential Information

3.5. "Confidential information" is any information which was given to the Trust in confidence or which is otherwise held under a duty of confidence. It includes personal confidential data (see next definition) and information which is commercially confidential. This policy does not use the wider definition of confidentiality used in the HSCIC Code of Practice on Confidential Information 2014 but has taken into account its recommendations.

Processing

3.6. Processing is any action whatsoever in relation to data from the moment of its creation to the moment of disposal or destruction. For the avoidance of doubt this includes both any act of consulting data and also simply holding data which is not, or unlikely to be, consulted.

Data Controller

3.7. A data controller is an individual, company or organisation that determines (sometimes in conjunction with others) the purpose and manner in which personal data may be processed. For the purpose of this policy the Trust is the primary data controller.

Data Subject

3.8. A living individual who is the subject of personal data

4. Responsibilities

4.1. Key responsibilities for Information Governance are set out in the Trust's Information Governance Policy. Of particular relevance to this policy are the Senior Information Risk Owner and Caldicott Guardian (see Information Governance Policy for further information on the SIRO roles.

Information Governance & IM&T Steering Committee

4.2. The Information Governance & IM&T Steering Committee supports the role of the Director of Finance & Performance and has a remit, on behalf of, and reporting to the Director to:

- Oversee the implementation and review of the Information Governance Policy and Framework and the Information Governance Strategy.
- Develop, approve and implement associated policies and procedures in relation to IG.
- Review and sign off the IG work programme.
- Ensure the accurate completion, review and sign off of the annual HSCIC Information Governance Toolkit assessment.

Information Governance Team

- Ensures that Caldicott, Data Protection and Freedom of Information principles are applied and promoted throughout the Trust and partnering organisations.
- Ensures progress towards satisfying the requirements of the HSCIC Information Governance (IG) Toolkit in relation to scrutiny of information disclosure and regulation, thus providing assurance to the Information Governance & IM&T Steering Committee.

Head of Information Governance

- Leads the Information Governance Team.
- Ensures that confidentiality incidents are recorded and investigated.
- Ensures that the Trust's performance is accurately recorded through administration of the HSCIC Information Governance Toolkit
- Ensures that appropriate awareness training on the principles of confidentiality and Information Governance is disseminated, communicated and made available to all staff

Caldicott Guardian

4.3. The Caldicott Guardian (the Medical Director holds this position) takes the lead role in the Trust on matters of Confidentiality, Information Disclosure and Human Rights relating to personal confidential data.

5. Confidentiality Policy

5.1. Northern Devon Healthcare NHS Trust and its staff will at all times comply with the law of confidentiality, the requirements of the Data Protection Act 1998 and the Human Rights Act 1998 so far as they affect confidentiality obligations and with the seven Caldicott principles which specify that the Trust should:

1. Justify the purpose(s) for using personal confidential data.
2. Only use it when absolutely necessary.
3. Use the minimum that is required.
4. Ensure that access is on a strict need-to-know basis.
5. Ensure that everyone understands his or her responsibilities.
6. Ensure that everyone understands and complies with the law.
7. Recognise that the duty to share information can be as important as the duty to protect patient confidentiality.

5.2. Further information about these principles will be found in the Information Governance Handbook. In support of the principles the Trust has appointed its Caldicott Guardian and will:

- provide staff with appropriate training to ensure that:
  - confidential information is used on a need-to-know basis and never disclosed to anyone who is not lawfully authorised to receive it;

- any unknown person who enters a ward or department and appears to be accessing or attempting to access confidential information should be challenged for proof of identity;
- confidential information whether paper or electronic is kept secure at all times from unauthorised access or use;

- Ensure that patients are made aware of any information sharing that must take place in order to provide them with high quality care, and will be told with whom the information is proposed to be shared. For example, clinical governance and clinical audit are components of healthcare provision, but this may not be clear to patients unless they are told or given information leaflets. This includes sharing between members of care teams from different organisations e.g. social services, hospice, & partner organisations with which the Trust runs shared clinical services.
- Not sanction the use of identifiable patient confidential data where the desired purposes can be achieved with anonymised or pseud-anonymised data. The Trust and its staff will have regard to the Information Commissioner's Anonymisation Code of Practice and the NHS Anonymisation Standard for Publishing Health and Social Care Data.
- Ensure that, where sharing or disclosure of identifiable patient confidential data takes place for non-care purposes e.g. research and invoice validation, this is done only with explicit consent unless there is a lawful basis for doing so, which shall be recorded together with the reasons for the decision to share or disclose.
- Maintain appropriate guidance for staff on the steps to be taken in compliance with this policy and in particular will maintain an index of "confidentiality decisions in practice which staff may consult". This guidance is contained in the Information Governance Handbook which will be published on the Trust's intranet and also on the internet in support of the Trust's commitments to openness and transparency.

5.3. In setting this policy the Trust has taken into account the recommendations in the HSCIC Code of Practice on Confidential Information 2014. The Trust and its staff (including temporary and agency) will comply with the 2003 NHS Confidentiality Code of Practice 2003. In addition, the Trust adopts and endorses the five rules of confidentiality contained within the 2013 HSCIC Guide to Confidentiality in Health and Social Care:

1. Confidential information about service users and patients will be treated both confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies and systems in place to ensure that the confidentiality rules are followed.

5.4. Further information about these rules and how they link with the Caldicott principles will be found in the Information Governance Handbook. They were developed by the HSCIC to support and enforce the principles as specifically recommended in the second Caldicott review.[1]

5.5. In support of the fifth rule the Trust will, in addition to this policy, maintain specific policies:

- For compliance with the NHS Information Security Code of Practice: IT security Policy
- For compliance with the NHS Records Management Code of Practice: Information Lifecycle Management Policy
- For compliance with the Data Protection Act 1998: Data Protection Policy
- For ensuring, where required, that patient consent is obtained and maintained for the use of identifiable patient confidential data: Consent Policy and Mental Capacity Act Policy

5.6. The Trust will ensure that confidentiality clauses will be built into staff and supplier contracts and all staff, volunteers, and contractors handling confidential information will be required to sign undertakings to comply with this policy.

5.7. The Trust respects and supports the privacy rights of its staff. This policy applies equally to personal confidential data about staff as it does to patient data. Nevertheless circumstances may arise where staff may feel that their privacy is being infringed, for example if a patient insists on recording a care visit. The Trust has produced a Code of Conduct which patients can be asked to conform to but, should they not do so, the duty to treat patients must take priority and it is likely that staff would be in breach of their own professional codes of conduct, and the obligations in their contract of employment, if they declined to provide treatment in such cases. Further guidance on this issue is available from the Care Quality Commission.

5.8. Readers of this policy must be aware however that neither the five Rules nor the seven Caldicott principles can be read as absolute. The legal framework allows for reasonableness, necessity and proportionality. For example an individual's right to object to sharing would be overruled by a duty to share or disclose information if this was necessary for the safeguarding of a vulnerable child or adult. In cases of doubt readers must consult the Codes referred to above, the Information Governance Handbook, and seek advice from the Information Governance team.

6. Compliance and Effectiveness

Standards / Key Performance Indicators

6.1. The key performance indicators will be number of:

[1] Recommendation 21: "The HSCIC's Code of Practice for processing personal confidential data should adopt the standards and good practice guidance contained within this report."

- Confidentiality related incidents reported on Datix.
- Data protection breaches reported to the ICO.

Implementation and Monitoring Compliance and Effectiveness

6.2. Monitoring compliance with this policy will be the responsibility of the Information Governance Team. This will be undertaken by reference to an annual work programme focussing on improvement recommendations arising from completion of the annual HSCIC IG Toolkit submission and other information governance initiatives, audits and external monitoring e.g. by CQC and Monitor.

6.3. This will include an annual programme of assessments and audits.

6.4. The Policy will be reviewed and re-approved every three years or sooner in the event of significant legislative changes.

6.5. Minor amendments and corrections between approvals may be made by the Head of IG (for example to reflect minor changes to legislation or national NHS requirements) subject to such consultation as may be appropriate e.g. with the Caldicott Guardian if relating to confidentiality issues. Such amendments will be published and reported to the Steering Committee at the first available opportunity, save that corrections which consist solely of updating external or internal hyperlinks need not be so reported.

7. Trust Core Values

7.1. This policy is designed to support and reinforce the Trust's five Core Values:

Act With Integrity	This policy requires and supports all staff to act with integrity within a defined legal and ethical framework when handling information.
Respect Diversity	This policy respects diversity by providing the same rights for all and ensuring that the wishes of the individual about the care of their information be respected
Demonstrate Compassion	This policy supports a compassionate approach to care by ensuring that the highest standards of confidentiality are maintained and that records, particularly patient records, are kept secure, accurate relevant and up to date
Listen and Support others	This policy supports patients by providing a framework within which their wishes in relation to their personal confidential data can be respected and upheld, and supports them should they wish to exercise their rights set out in the NHS Care Records Guarantee.
Strive for Excellence	This policy adopts and endorses the highest standards of behaviour, and of the management of information, by incorporating all relevant national standards and professional Codes of Practice

8. Equality Impact Assessment

8.1. The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. An Equality Impact Assessment Screening has been undertaken and there is one positive impact

Table 1: Equality impact Assessment

Group	Positive Impact	Negative Impact	No Impact	Comment
Age			X	
Disability			X	
Gender			X	
Gender Reassignment			X	
Human Rights (rights to privacy, dignity, liberty and non-degrading treatment), marriage and civil partnership	X			Applicable to all under Human Rights Legislation
Pregnancy			X	
Maternity and Breastfeeding			X	
Race (ethnic origin)			X	
Religion (or belief)			X	
Sexual Orientation			X	

9. References

9.1. Where possible, references have been linked in the body of this policy. The following additional references are also relevant to data protection compliance.

- Access to Medical Reports Act 1988
- Handbook to the NHS Constitution 2013
- Caldicott Guardian Manual 2010

10. Associated Documentation

10.1. Supporting this policy are a number of topic specific policies and strategies, and associated guidance.

- Consent Policy
- Mental Capacity Act Policy
- Data Protection Policy
- Healthcare Records Policy
- Information Security Policy
- Information Lifecycle Management Policy
- Information Governance Handbook

11. Appendix A - Glossary of Terms and Abbreviations

Note: See also Section 3 – Definitions and the HSCIC IG Toolkit Glossary of Terms.

Term / Abbreviation	Explanation
CG	Caldicott Guardian - See Section 4.3
CQC	Care Quality Commission. The safety and quality regulator (or watchdog) of healthcare and adult social care services
DoH	Department of Health
DPA	Data Protection Act 1998
EIR	Environmental Information Regulations 2000
FOI(A)	Freedom of Information (Act) 2000
HSCIC	Health & Social Care Information Centre
IAO	Information Asset Owner
IAA	Information Asset Administrator
ICO	Information Commissioner's Office
IG	Information Governance
IM&T	Information Management and Technology
Monitor	The independent regulator for NHS Foundation Trusts.
NDDH	North Devon District Hospital
NDHT / The Trust	Northern Devon Healthcare NHS Trust
PCD	Personal Confidential Data
Staff	In general the duties of compliance in this policy apply to all staff including temporary agency and volunteers and 'staff' should be interpreted accordingly. Special arrangements may apply in a limited number of areas e.g. around training.

12. Appendix B: Recommendations of the Information Governance Review (Caldicott2)[2]

No.	Recommendation	Trust Position at June 2015
2	For the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual. Health and social care providers should audit their services against NICE Clinical Guideline 138, specifically against those quality statements concerned with sharing information for direct care.	The Trust undertakes patient surveys which measure some or all of the guidance and also takes into consideration results of the mandatory national patient surveys. The Trust takes appropriate action according to the patient feedback received. The approach to NICE Clinical Guideline 138 will be further reviewed in the light of changes to the IG Toolkit in version 13.
4	Direct care is provided by health and social care staff working in multi-disciplinary 'care teams'. The Review recommends that registered and regulated social workers be considered a part of the care team. Relevant information should be shared with members of the care team, when they have a legitimate relationship with the patient or service user. Providers must ensure that sharing is effective and safe. Commissioners must assure themselves on providers' performance. Care teams may also contain staff that are not registered with a regulatory authority and yet undertake direct care. Health and social care provider organisations must ensure that robust combinations of safeguards are put in place for these staff with regard to the processing of personal confidential data.	This Confidentiality Policy recognises this requirement. It explicitly adopts the new seventh Caldicott Principle. It explicitly adopts the Second Rule in the HSCIC Guide to Information Sharing in Health & Social Care: "Members of a care team should share confidential information when it is needed for the safe and effective care of an individual". All relevant data flows will be identified and risk managed as part of the Trust's Information Asset Register processes
5	In cases when there is a breach of personal confidential data, the data controller, the individual or organisation legally responsible for the data, must give a full explanation of the cause of the breach with the remedial action being undertaken and an apology to the person whose confidentiality has been breached.	The Trust's Raising Concerns and Complaints Policy applies. This requires *"Clear apologies where expectations have not been met or where there have been shortcomings."* It also commits to *"Provide a full and honest explanation of all points raised".*
6	The processing of data without a legal basis, where one is required, must be reported to the board, or equivalent body of the health or social care organisation involved and dealt with as a data breach. There should be a standard severity scale for	The Trust has a clear Incident management Policy which meets this requirement and adopts NHS guidance for managing incidents including SIRI's

[2] The Information Governance Review: To Share or Not to Share March 2012

No.	Recommendation	Trust Position at June 2015
	breaches agreed across the whole of the health and social care system. The board or equivalent body of each organisation in the health and social care system must publish all such data breaches. This should be in the quality report of NHS organisations, or as part of the annual report or performance report for non-NHS organisations.	
7	All organisations in the health and social care system should clearly explain to patients and the public how the personal information they collect could be used in de-identified form for research, audit, public health and other purposes. All organisations must also make clear what rights the individual has open to them, including any ability to actively dissent (i.e. withhold their consent).	The Trust has a Patient Information Leaflet. This is due for review in 2015 and will be assessed to ensure it takes into account developments in this area, this policy and the various Codes of Practice.
19	All health and social care organisations must publish in a prominent and accessible form: • a description of the personal confidential data they disclose; • a description of the de-identified data they disclose on a limited basis; • who the disclosure is to; and • the purpose of the disclosure.	The Trust's Information Governance Policy (2015) contains a commitment that "The public, including patients, will be told how information about them is used, and about safeguards governing use of personal data." In fulfilling this commitment the Trust will review its website and in particular the Freedom of Information Publication scheme to ensure that this recommendation is addressed.
22	The information governance advisory board to the Informatics Services Commissioning Group should ensure that the health and social care system adopts *a single set of terms and definitions relating to information governance that both staff and the public can understand. These terms and definitions should begin with those set out in this document.* All education, guidance and documents should use this terminology	In section 2 of the Information Governance Policy and Framework the Trust commits to using standard terms.
25	The Review Panel recommends that the revised Caldicott principles should be adopted and promulgated throughout the health and social care system.	The Trust has adopted the revised principles in this edition of this policy and in associated policies (Consent, Data Protection, Information Governance) and will undertake an appropriate awareness programme once the policies have been approved an published, along with an Information Governance Handbook.