The Pennine Acute Hospitals NHS Trust

INFORMATION SHARING PROTOCOL AGREEMENT PROCEDURE

(TIER 1 AND TIER 2)

Pennine Acute Hospitals NHS Trust

&

Bury MBC, Manchester City Council, Oldham and Rochdale MBC

May 2012

Standard Operating Procedure:	**INFORMATION SHARING AGREEMENT PROCEDURE (TIER 1 AND TIER 2)**
Version No:	1.0
Date this version approved:	May 2012
Author(s) (Job title)	Trish Noon Information Governance Manager Pennine Acute Hospitals NHS Trust
Division/Directorate	INFORMATION GOVERNANCE/IM&T
Trust wide SOP (Yes/No)	YES
Links to other Policies, SOP's, Strategies etc:	Information Governance Policy

Date(s) previous version(s) approved (if known)**:**	**Version: N/A**	**Date: N/A**
Date of Next Review	**May 2014**	
Manager Responsible for Review:	Head of Midwifery	

Information Sharing Agreement & Procedure

Between: Pennine Acute Hospitals NHS Trust

And: Bury MBC, Manchester City Council, Oldham and Rochdale MBC

For: The notification of pregnancies and subsequent births to Children's Centres, **with pregnant woman's consent.**

AT ALL TIMES, STAFF MUST TREAT EVERY INDIVIDUAL WITH RESPECT AND UPHOLD THEIR RIGHT TO PRIVACY AND DIGNITY.

1.0 INTRODUCTION

This Information Sharing Agreement (ISA) Procedure provides information on 'who, what, when, where, why and how' personal data is to be shared between the parties to this agreement. Local organisations are increasingly working together. In order to work effectively and efficiently, organisations need to be able to share information about the service they provide and the people they provide these services to.

This agreement covers the sharing of personal identifiable data (PID), with the individual's **express consent**, unless a legal or statutory requirement applies for the following purposes:

- Provision of appropriate care services
- Improving the health of the population
- Protecting people and communities
- Supporting people in need
- Supporting legal and statutory requirements
- Managing and planning services (where information has been suitably anonymised)
- Commissioning and contracting services (where information has been suitably anonymised)
- Developing inter-agency strategies
- Performance management and audit
- Research (subject to the Research Governance Framework)
- Investigating complaints or serious incidents
- Reducing risk to individuals, service providers and the public as a whole
- Clinical Audit
- Monitoring and protecting public health
- Common Assessment Framework
- Staff management and protection
- To fulfil responsibilities in law such as; Data Protection Act (1998), Human Rights Act (1998), Common Law, Crime and Disorder Act (1998), Mental Health Act (1983), Fertilisation and Embryology Act (1990), NHS (Venereal Diseases) 1974 Regulations and the Children Act (2004).

This is not intended to be an exhaustive list. If, as a result of policy changes or other developments, additional information sharing requirements arise these will be added to the protocol.
This protocol does not give carte blanche licence for the wholesale sharing of information. Information sharing must take place within the constraints of the law and relevant guidance and service specific requirements.

The needs and responsibilities of all partner organisations are clearly outlined within this ISA.

2.0 SCOPE

This ISA details the specific purpose(s) for information sharing, the group(s) of service users it impacts upon, the relevant legislative powers, what data is to be shared, the consent processes involved (where appropriate), the required operational procedures and the process for review.

In order to share information between partners there must be a defined and justifiable lawful purpose(s) which supports the effective delivery of a policy or service that respects people's expectations about the privacy and confidentiality of their personal information but also considers the consequences of a failure to act.

The partners to this agreement may only use the information disclosed under this information sharing arrangement for the specific purpose(s) set out in this document. They may not regard shared information as intelligence for the general use of their organisation unless they have defined and agreed the purpose within the ISA and have informed the respective service users of this change of use.

3.0 PARTIES TO THE ISA

The Caldicott Guardian (or equivalent Director) in each of the participating organisations will be required to sign up to a Tier 1 Overarching Information Sharing Agreement as a minimum standard (appendix 1), prior to acceptance of this Tier 2 Information Sharing Agreement.

Organisations participating in this Tier 2 information sharing agreement are those that have signed the Declaration of Acceptance and Participation (DAP) at the end of this document (Appendix 4). The Declaration of Acceptance, provides details of each organisation's 'Designated Person(s)' and will be updated and reissued as and when any changes are necessary or required. The List of Designated Data Sharing Personnel (Appendix 5) also needs to be completed. This details those personnel whom data is transferred to and from for each partner organisation.

The Caldicott Guardian (or equivalent) will be required to sign this agreement on behalf of the participating organisation. By signing this document each organisation agrees to accept this ISA and to adopt the statements and procedures contained within it and any associated documents arising out of it.

Amendments to the principles of this ISA will only be sanctioned with the knowledge and approval of all of the participating organisations.

It is the responsibility of the Manager(s), and/or 'Designated Person(s)', who have negotiated and agreed this ISA to produce any associated 'Operational Instruction(s)' Tier 3 arrangements and to ensure dissemination and implementation.

Each of the Partner organisations will be held personally responsible for maintaining the security of the shared information held in any electronic systems or manual files within that organisation in keeping with Principle 7 of the Data Protection Act 1998.

Where a partner organisation or employee is responsible for any loss / misappropriation / misuse of the data shared under this agreement they will be subject to any penalties imposed by law in relation to that loss.

Further, individuals who misuse data will be subject to disciplinary arrangements within their own organisations.

Partner organisations must declare any proposed processing of the shared information outside of the European Economic Area prior to any transfer.

4.0 CONFIDENTIALITY, CONSENT AND INFORMATION SHARING PRINCIPLES

It is the responsibility of the manager(s), and/or 'Designated Person(s)', negotiating and agreeing this ISA to always have consideration of its impact on the privacy and confidentiality of service users and to take account of their legitimate expectations and rights in regard to the use of that individual's personal information.

Organisations will endorse, support and promote the accurate, timely, secure and confidential sharing of both person identifiable and anonymised information where such information sharing is essential for the care and treatment of patients.

Organisations are fully committed to ensuring that if they share information it is in accordance with their legal, statutory and common law duties, and, that it meets the requirements of any additional guidance.

Patients will be fully informed about information that is recorded about them and as a general rule, be asked for consent before their information is shared with colleagues of another organisation unless anonymised.

The rules about disclosure apply to patients who lack capacity. Where appropriate, consent should be obtained from the person with legal authority to act on the person's behalf. The reasons for final decision should be clearly recorded.

Where professionals request that information supplied by them be kept confidential from the people who use the services, the outcome of this request and the reasons for taking the decision will be recorded.

Information will not be used for any other purposes of further shared without the prior consent of the patient other than what is stated in this agreement.

All signatories to this agreement have in place policies and procedures to meet the national requirements for Data Protection, Information Security and Confidentiality. The existence of, and adherence to, such policies provides all agencies with confidence that information shared will be transferred, received, used, held and disposed of appropriately.

Both organisations will ensure that all relevant staff are aware of, and comply with, their responsibilities in regard to both the confidentiality and security of information.
All staff must be made aware that disclosure of personal information, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally, could be subject to disciplinary action.

Organisations are responsible for putting in place effective procedures to address complaints relating to the disclosure of information, and information about these procedures should be made available to patients.

Organisations acknowledge their 'Duty of Confidentiality' to the people they serve. In requesting release and disclosure of information from other agencies employees and any other personnel associated wit this service will respect this responsibility and to seek to override the procedures which each organisation has in place to ensure that information is not disclosed illegally or inappropriately. This responsibility also extends to third party disclosures; any proposed subsequent re-use of information which I sourced from another agency should be approved by the source organisation.

An individuals' personal information will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary. For all other purposes information should be anonymised. Where it is agreed that the sharing of information is necessary, only that which is needed and relevant will be shared and that would only be on a "need to know" basis.

5.0 PURPOSE OF INFORMATION SHARING

WHERE THE PREGNANT WOMAN HAS GIVEN HER CONSENT, Information will be shared between organisations to:

FACILITATE RAPID AND TIMELY ACCESS TO THE UNIVERSAL PROVISION OF PARENTING SUPPORT PROVIDED BY LOCAL AUTHORITIES WITHIN THE SPIRIT OF THE UNIVERSAL HEALTHY CHILD PROGRAMME (PROGRAMME COVERS PREGNANCY TO 19 YEARS),

6.0 LEGAL BASIS FOR INFORMATION SHARING

- Access to Health Records Act 1990
- Access to Medical Reports 19988
- Children Act 2004
- Common Law Duty of Confidentiality
- Crime and Disorder Act 1998
- Criminal Justice and Police Act 2001
- Data Protection Act 1998
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- Education Act 2002
- Freedom of Information Act 2000
- Human Rights Act 1998
- Mental Health Act 2007
- Mental Capacity Act 2005
- Protection of Children Act 2005
- Special Educational Needs and Disability Act 2001
- Youth Justice and Criminal Evidence Act 1999

7.0 INFORMATION SHARING PROCEDURES AND PROCESSES

7.1 Appendix 1 Information Sharing Protocol

Appendix 2 Data Flows indicates the data items that may be shared, methods and frequency of transfer of data within the boundaries of this agreement and in the best interests of the patient.

Appendix 3 Declaration of Acceptance and Participation indicates the data sharing processes identifying contacts within organisations.

7.2 Methods of Recording and Holding Information

Data must be recorded on the organisations electronic database or held in "relevant filing systems," to maintain contemporaneous records, and to enable legitimate processing in accordance with the Data Protection Act 1998.

Data will not be used for any other purpose other than the purpose stated in this agreement in compliance with Principle 2 of the Data Protection Act 1998.

Information will be kept accurate and up to date to comply with Principle 4 of the Data Protection Act 1998.

Retention of data will be in accordance with each individuals organisations retention schedule and / or the Records Management NHS Code of Practice.

7.3 Access to Information

Where any of the partners to this agreement has a legitimate need to share or transfer relevant personal data with any 3rd party processor or contractor, Principle 7 of the Data Protection Act 1998 will apply and a current ISA must be in place and an up to date Data Protection Registration/Notification must be in place with the Information Commissioners Office.

In order to access personal data all relevant staff under this agreement and any sub-contractors must have a current CRB check.

Personal information relating to all individuals associated with this agreement is subject to the Common Law Duty of Confidentiality. Partner organisations should ensure that employees attend training on confidentiality, data protection and the security of information.

Contracts of employment should reflect confidentiality, information security and disciplinary action in the event of inappropriate access to or misuse of personal identifiable information.

Information should only be accessed by those who are directly involved in the care of that individual or for the purposes of monitoring statistical or quality standards.

7.4 Other Information (Not in the Data Items Table)

Where there is a need to share information on an ah-hoc basis, or information that is not listed in Appendix 1, consent must be gained from the data subject prior to the exchange of the information or where there seems to be an overriding need to ensure the safety and / or wellbeing of any data subject. Wherever possible, consent must be gained from the data subject prior to the information exchange.

8.0 HUMAN RIGHTS ACT 1998

There are implications arising from the Human Rights Act 1998 which imposes a duty on all public bodies to act consistently with the European Convention on Human Rights. In particular, Article 8 (Right to Respect for Private and family life). Providing staff comply with their duty of confidentiality as set out in the Data Protection Act 1998 and their common law duty of confidentiality their activities should fall within the requirements set out in the European Convention of Human Rights

9.0 MONITORING AND REVIEW

Compliance with this agreement will be monitored by a review of the information sharing arrangements with partner organisations and as per the Information Governance Toolkit requirements.

Appendix 1. **Information Sharing Protocol** - Tier 1

Between: **Pennine Acute Hospitals NHS Trust**

And: **Bury MBC, Manchester City Council, Oldham and Rochdale MBC**

This is an overarching protocol to enable the above organisations to govern information sharing, thereby ensuring seamless pathways of care for the service user. It provides a framework for safeguarding the processing of all personal information.

The protocol will be supplemented in some circumstances by individual protocols (Tier 2) for specific service areas. These will set out detailed purposes and operational procedures for the sharing of information. It should also be read in conjunction with staff guidelines on the transfer of personal information.

General Principles

1. Each organisation signing this protocol shall have appointed a responsible officer who will ensure the protection of personal information e.g. Caldicott Guardian or senior manager responsible for data protection.
2. Each organisation signing this protocol will be taking appropriate measures towards compliance with Data Protection Act 1998 and the Caldicott Principles, ISO 17799 / Information Security Management: NHS Code of Practice, Records Management: NHS Code of Practice and national guidance and rules around holding and destroying health/social services records and other relevant legislation.
3. Each organisation is committed to reviewing practice with the aim of ensuring all exchanges of personal information meet legal and Caldicott standards.
4. Each organisation is committed to ensuring staff are appropriately trained in data protection/Caldicott procedures.
5. Each organisation is committed to issuing practical guidelines to staff on the transfer of personal information.

Signed by:

Signature Print name Dr Sally Bradley Date
Pennine Acute Hospitals NHS Trust Caldicott Guardian.

Signature Print name **Saul Ainsworth** Date
Bury Children's Caldicott Guardian

Signature Print name **Bridget Keane** Date

Manchester Children's Caldicott Guardian

Signature Print name **Lesley Perkins** Date

OLDHAM Caldicott Guardian

Signature Print name **Colin Foster** Date

Rochdale Caldicott Guardian

Appendix 2 **INFORMATION SHARING PROTOCOL - Tier 2 Data Flows**

N.B. **The data will be shared only with the pregnant woman's consent.**

Description of Data / Information to be shared.	**From and To**	**Purpose of Sharing Information**	*** Data Items**	**Frequency & Method of Information Transfer.** e.g. Safe Haven Fax, Encrypted email sent via nhs.net etc.
Ante-Natal	From PAHNT Vicky Brooks Euroking Information Asset Administrator (System Manager) **TO** **BURY** - Syeed Ismail S.Ismail@bury.gcsx.gov.uk **MANCHESTER** - Liz Crix L.Crix@manchester.gcsx.gov.uk **OLDHAM** Ian McLaren ian.mclaren@oldham.gcsx.gov.uk **ROCHDALE** Tanya Firth tanya.firth@rochdale.gcsx.gov.uk	To enable Children's Centres to target services and provide support to pregnant mothers. Information to be shared only with explicit consent. Consent to be recorded on Euroking system.	1, 3 and 4 Forename, Surname, Address, Postcode, D.O.B. Tel Number. Expected Date of Delivery for this pregnancy.	Monthly via secure e-mail transfer.
Post-Natal	From **PAHNT** Community Midwifery Clerks **TO** **BURY** Children's Centres, Childcare and Early Years Team (CCCCEY) **MANCHESTER** Sure Start and Early Years Children's Services **OLDHAM** Information Analyst Performance, Services and Capacity **ROCHDALE** Performance & Transformation Service Sure Start Data Team	To enable Children's Centres to target services and provide support to mothers and children.	Duplicate page extracted from Red Book - 1, 2, 3 and 4 Child's Name Gender, Ethnicity, D.O B and NHS No. Name of Local Children's Ctr ,Tel No & Address Name of Person Giving Consent Signature & Date Name of Mum & Dad DOB and Ethnicity. *(If appropriate name of other carer and address).* Mum and Dads contact Tel Nos. Professional Name completing form and designation.	Weekly Delivery by Trust distribution department.

Data Flow Approved by Information Asset Owner (PAHNT Divisional Director)
Name _Cathy Trinick _

Signature _____ **Date** _____

Job Title _____

Data Items Key:

1. Personal
2. Personal/Sensitive
3. Clinical /Sensitive
4. Demographic
5. Other

Definition of *Data Items

No.	***Data Item***	**Definition**
1	**Personal**	Name Date of birth Next of kin Personal circumstances NHS Number Financial information Physical description Gender
2	**Personal/Sensitive**	Racial/ethnic origin Religion Trade Union membership Court proceedings Criminal convictions Political opinions Physical or Mental Health
3	Clinical/Sensitive	Information relating to physical or mental health or condition
4	**Demographic**	Address Postcode Telephone number Location description Directions
5	**Other**	Environmental Social Health professional

Appendix 3 Declaration of Acceptance and Participation (DAP)

Signed by, for and on behalf of: Pennine Acute Hospitals NHS Trust

CALDICOTT GUARDIAN - PAHNT			
Data Protection Act ICO Registration No: :	**Z6519461**	**Renewal Date:** March 2014	
Name:	**Dr Sally Bradley**		
Position:	**Caldicott Guardian**		
Email Address	Sally.bradley@pat.nhs.uk		
Signature:		**Date:**	

Signed by, for and on behalf of: Bury MBC

CALDICOTT GUARDIAN - BURY			
Data Protection Act ICO Registration No:	**Z5720815**	**Renewal Date: October 2012**	
Name:	**Saul Ainsworth**		
Position:	**Caldicott Guardian**		
Email Address	s.ainsworth:bury.gov.uk		
Signature:		**Date:**	

Signed by, for and on behalf of: MANCHESTER CITY COUNCIL

CALDICOTT GUARDIAN - MANCHESTER			
Data Protection Act ICO Registration No:	**Z6942262**	**Renewal Date: July 2012**	
Name:	**Bridget Keane**		
Position:	**Caldicott Guardian**		
Email Address	**b.keane@manchester.gov.uk**		
Signature:		**Date:**	

Signed by, for and on behalf of: OLDHAM MBC

CALDICOTT GUARDIAN - OLDHAM			
Data Protection Act ICO Registration No:	**Z6904132**	**Renewal Date: 29th July 2012**	
Name:	Lesley Perkins		
Position:	**Caldicott Guardian**		
Email Address	lesley.perkins@oldham.gov.uk		
Signature:		**Date:**	

Signed by, for and on behalf of: ROCHDALE MBC

CALDICOTT GUARDIAN - ROCHDALE			
Data Protection Act ICO Registration No:	**Z5481774**	**Renewal Date: 1st November 2012**	
Name:	**Colin Foster**		
Position:	**Caldicott Guardian**		
Email Address	**Colin.foster@rochdale.gov.uk**		
Signature:		**Date:**	

Appendix 4 List of Designated Data Sharing Personnel

Partnership Member	Designated Person and Position Held	Contact Details
Pennine Acute Hospitals NHS Trust	Vicki Brooks RM Euroking Maternity Information Asset Administrator (System Manager).	**Address:** Vicki Brooks RM Link IT Midwife Ante Natal Clinic Maternity Computer Studies Office Royal Oldham Hospital Rochdale Road Oldham OL1 2JH **Telephone No:** 0161 778 5174 **Secure Email:** Vicki.brooks@nhs.net
BURY MBC	Syeed Ismail	**Address:** Children's Centres, Childcare and Early Years Team (CCCCEY) 1st Floor Athenaeum House Market Street Bury BL9 0BN **Telephone No:** 0161 253 7429 **Secure Email:** S.Ismail@bury.gcsx.gov.uk
MANCHESTER MBC	Liz Crix	**Address:** Liz Crix, Children's Services (Early Years) Manchester City Council POSTAL ADDRESS: P.O. Box 532, Town Hall Manchester M60 2LA LOCATION ADDRESS: 3rd Floor, Number One First Street Manchester M15 4FN (use M1 5DE for sat nav) **Telephone No:** 0161 234 1496 (internal prefix 800) **Secure Email:** L.Crix@manchester.gcsx.gov.uk
OLDHAM MBC	Ian McLaren	**Address:** Ian McLaren Information Analyst Performance, Services and Capacity Oldham Council Room 435 Civic Centre West Street Oldham OL1 1XJ **Telephone No:** 0161 770 1328

		Secure Email: **ian.mclaren@oldham.gcsx.gov.uk**
ROCHDALE MBC	Tanya Firth	**Address:** Performance & Transformation Service Sure Start Data & Monitoring Manager Sure Start Data Team Floor 2, Crossfield Mill, Crawford St Rochdale OL16 5RX **Telephone No:** 0844 225 0322 **Secure Email:** **tanya.firth@rochdale.gcsx.gov.uk**

Appendix 5 References and further information

Legal Framework

The Trust is bound by the provisions of a number of items of legislation and regulation affecting the stewardship and control of information. The main relevant legislation are:

- Data Protection Act 1998
- Computer Misuse Act 1990
- Children Act 1989 & 2004
- Copyright, Designs and Patent Act 1988
- Copyright (Computer Programs) regulations 1992
- Environmental Information Regulations 2004
- Health & Social Care Act 2001
- NHS Act 2006
- Freedom of Information Act 2000
- Human Rights Act 1998
- Human Fertilisation and Embryology Act 1990
- Abortions Regulations 1991
- Access to Health Records Act 1990
- Crimes & Disorder Act 1998
- Public Interest Disclosure Act 1998
- Public Records Act 1958
- Regulations under the Health and Safety at Work Act
- Electronic Communications Act 2000
- Regulations of Investigatory Powers Act 2000
- NHS Trust and Primacy Care Trusts (Sexually Transmitted Diseases) Directions 2000
- Re-use of Public Sector Information Regulations 2005

This list is not exhaustive.

Regulatory Framework

In relation to many of the above, the NHS has set out and mandated a number of elements in regulation that constitute “Information Governance” through a national programme. This area is developing at a fast changing pace and the focus within this section will need significant periodical review.

The Regulatory Elements are:

- The Information Governance Toolkit requirements in particular requirement 302 which asks are there documented information security incident / event reporting and management procedures that are accessible to all staff
- Caldicott Report 1997 and Caldicott Principles– a report for the audit and improvement on the use of patient identifiable data
- Checklist for Reporting, Managing and Investigating IG SUI’s – Department of Health (2010)
- Confidentiality: NHS Code of Practice (2003)
- The Caldicott Guardian Manual 2010
- Records Management: NHS Code of Practice (2007)
- Information Security Management: NHS Code of Practice (2007)
- NHS Information Governance Guidance on Legal and Professional Obligations (2007)
- Guidance for Access to Health Records Requests (2010)
- Information Quality Assurance / Data Standards requirements
- Information Commissioner requirements
- NHS Complaints Policy (2009)
- NHS Information Risk Management

Policies & Procedures

- Access to Health Records Policy
- Confidentiality Code of Conduct
- Corporate Records Management Policy
- Data Protection Policy
- Data Quality Policy
- Freedom of Information Policy
- Fax Machine Policy
- Information Governance Booklet for staff
- Information Governance Policy
- Information Risk Policy
- Incident Reporting Policy and Procedure
- Use, Consent and Disclosure of Information Policy
- Laptops, Portable IT Equipment and Removable Computer Media Policy (IT Services)
- Disciplinary Policy (Human Resources)
- Safe Haven Policy
- Employee Personal Files Policy (Human Resources)
- (Whistle Blowing) Open Door Policy for Handling Staff Concerns
- Use, Consent and Disclosure of Information Policy
- Raising Concerns Policy and Procedure
- Complaints Policy

Appendix 6

Glossary of Terms

Audit
An official inspection, or evaluation, e.g. that the organisation's processes are being complied with.

Bulk Personal Identifiable Data
The term 'bulk' is used to describe information relating to 51 or more individuals.

Business Critical Information
Where data loss of data would have a significant impact on the performance, reputation and operational effectiveness of the organisation. This may include but is not limited to data that is financial, personal, or relates to major projects.

Caldicott Guardian
A designated health or social care professional (usually a senior manager) responsible for ensuring that the (Caldicott) principles governing the sharing of patient-identifiable information are adhered to within their organisation

Classes
These are the groupings that information in the publication scheme is divided in to. They have been set by the Information Commissioners Office as part of the model scheme that an organisation has to adopt.

Disclosure logs
These are copies of previous responses we've sent out to people making requests under the Freedom of Information Act. We publish those that we believe may be of interest to a wider audience.

DPA - Data Protection Act 1998
The Data Protection Act gives individuals a right to access personal information held only about themselves. It is important the personal data is not given to a third party without prior consent.

Duty of Confidence
A duty of confidence arises when one person discloses information to another (eg patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation that is derived from case law.

Encryption
The process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Exemptions
These are set out in the legislation and are the legal reasons why an organisation may decide not to release information to an individual upon request. Exemptions fall into two categories; non-qualified and qualified. When a qualified exemption applies the organisation must undertake a public interest test.

FOI - Freedom of Information Act 2000
The Freedom of Information Act came into force in January 2005 and is intended to make information held by public authorities available to the public to demonstrate transparency and encourage openness.

Information Asset
Operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, records and information.

Information Asset Administrators (IAA)

Information Asset Administrators are usually operational members of staff who understand and are familiar with information risks in their area or department, eg. Security Managers, Records Managers, Data Protection Officers, Internal Audit. For smaller organisations, an appropriate operational role may include Office or Departmental Managers, Shift Supervisors and senior administrative staff. Information Asset Administrators will implement the organisation's information risk policy and risk assessment process for those information assets they support and will provide assurance reports to the relevant Information Asset Owner as necessary.

Information Asset Owners (IAO)
Information Asset Owners are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. Information Asset Owners may be assigned ownership of several assets of their organisation.

Information Commissioners Office (ICO)
The Information Commissioners Office is the regulator responsible for ensuring that organisations covered by the FOI Act adhere to the legislation. For more details visit the Information Commissioners Office website.

Information Governance Framework
The information governance framework for health and social care is formed by those elements of law and policy from which applicable information governance standards are derived, and the activities and roles which individually and collectively ensure that the set standards are clearly defined and met. Whilst a key focus of information governance is the use of information about service users, it applies to information and information processing in its broadest sense and underpins both clinical and corporate governance.

Information Governance Incident
An information governance or information security related incident relates to breaches of security and / or the confidentiality of personal information which could be anything from users of computer systems sharing passwords, to a piece of paper identifying a patient being found in the high street. The severity level is rated from 0 – 2 according to the Checklist for Reporting, Managing and Investigating IG SUI's (Department of Health, Jan 2010).

Information Governance Serious Untoward Incident
An information governance or information security related incident relates to breaches of security and / or the confidentiality of personal information which could be anything from users of computer systems sharing passwords, to a piece of paper identifying a patient being found in the high street. The severity level is rated from 3 – 5 according to the Checklist for Reporting, Managing and Investigating IG SUI's (Department of Health, Jan 2010).

Information Governance Statement of Compliance
An agreement between NHS Conecting for Health and any organisation wishing to use services providing through the National Programme for IT. The agreement stipulates the obligations which the organisation is expected to maintain to ensure patient data is safeguarded and only used appropriately.

Information Lifecycle Management
Refers to the management of information throughout its lifecycle; from the point of its creation through to its eventual disposal.

Information Security
Protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

NHS Number
A national number assigned to all patients registered with the NHS in England and which is used by the NHS and social care as a unique patient identifier.

NHSmail

NHSmail is a secure national email and directory service used to transmit email messages between NHS organisations.

Non-Care Purpose
The use of information for a purpose that does not directly contribute to the diagnosis, care and treatment of an individual, or to the audit/assurance of the care provided.

Patient Identifiable Information
Any information that may be used to identify a patient directly or indirectly. Key identifiable information includes patient name, address, date of birth, full post code, images, tapes, NHS number and local identifiable codes.

Personal Data
Information relating to a living individual who can either be identified from that information on its own or from that and other information available to the Data Controller (see Client Identifiable Information). Personal data cannot be processed unless at least one of the conditions in Schedule 2 of the Data Protection Act 1998 is met (See Appendix 1). http://www.legislation.gov.uk/ukpga/1998/29/schedule/2

Public Authorities
The Freedom of Information Act only applies to public authorities as defined in the Act and includes companies that are wholly owned by public authorities.

Public interest test
The public interest test favours disclosure where a qualified exemption applies. In such cases, the information may be withheld only if the public authority considers that the public interest in withholding the information is greater than the public interest in disclosing it.

Publication scheme
The publication scheme sets out the information that the public authority makes routinely available, and assists the public in finding the information required.

Records Management
Records management is the practice of maintaining the records of an organisation from the time they are created up to their eventual disposal. This may include naming, version control, storing, tracking, securing, and destruction (or in some cases, archival preservation) of records.

Records Management: NHS Code of Practice
A guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on legal requirements and professional best practice.

Risk Management
Structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating, and controlling responding to risk.

Role-Based Access Control
Grants a view of a patient's record depending on the role the individual was assigned when they registered for access to the NHS Care Records Service and related IT services. Authorised users are only able to access the information they need to carry out their role, eg a booking clerk will see less information than a doctor.

Round Robin
A letter/email which has been sent to multiple recipients.

Safe Haven
A location (or system) within an organisation where arrangements and procedures are in place to ensure personal information can be held, received and communicated securely.

Sensitive Data
Data held about an individual which contains both personal and sensitive information. There are only seven types of information detailed in the Data Protection Act 1998 that are deemed as sensitive:

- racial or ethnic origin
- religious or other beliefs
- political opinions
- trade union membership
- physical or mental health
- sexual life
- criminal proceedings or convictions

Sensitive data detailed in the Data Protection Act 1998 cannot be processed unless at least one condition from both Schedule 2 and Schedule 3 are met. (see Confidential Data) (See Appendix1)

Senior Information Risk Owner (SIRO)
An Executive Director or member of the Senior Management Board with overall responsibility for the organisation's information risk policy. The SIRO will also lead and implement the information governance risk assessment and advise the Board on the effectiveness of risk management across the organisation.

Vexatious request
A vexatious request is one that is intended to cause distress, disruption or irritation. Under these circumstances an organisation can refuse to handle requests that may be considered to fall under this guidance.

Working days
It is important to remember that organisations have 20 working days in which to respond to an FOI request. Working days do not include the weekends or public holidays in the UK