Lincolnshire Partnership NHS
NHS Foundation Trust

Lincolnshire Partnership NHS Foundation Trust

Information Management & Security Policy

DOCUMENT VERSION CONTROL	
Document Type and Title:	**Information Management & Security Policy**
Authorised Document Folder:	**IM&T**
New or Replacing:	**Replacing version 4 of INFO1**
Document Reference:	**IM&T 1**
Version No:	**2 (Final)**
Date Policy First Written:	**February 06**
Date Policy First Implemented:	**March 2006**
Date Policy Last Reviewed and Updated:	**January 2011**
Implementation Date:	**November 2012**
Author:	**Steve Lidbetter, Deputy Director of Performance and Information**
Approving Body:	**IM&T Committee**
Approval Date:	**November 2012**
Committee, Group or Individual Monitoring the Document	**Information Governance Group**
Review Date:	**November 2013**

Contents

1. Introduction

2. Purpose

3. Duties

4. Definitions

5. Legislation

6. Policy Framework

7. Audit and Monitoring

8. Policy Approvals

9. References

10. Appendices

1. Introduction

1.1 This top-level information security policy is a key component of Lincolnshire Partnership NHS Foundation Trust's overall information management and security framework and should be considered alongside more detailed information security documentation including, system level security procedures, security guidance and protocols.

1.2 Lincolnshire Partnership NHS Foundation Trust is a mental health and social care Trust providing services across Lincolnshire, Derbyshire and North East Lincolnshire from over 70 sites. This includes a range of inpatient services and community based services. The Trust has approximately 2000 staff who, either work in direct care delivery or provide a business support function (corporate services).

1.3 Information is collected and recorded in a number of mediums including paper and electronic. The Trust has well developed infrastructures and arrangements to support information security. It shares some of these arrangements with other health care providers (NHS and Non-NHS) and has developed shared care, memorandums of understanding and information sharing protocols with these organisations. Where these are identified as part of a contractual arrangement linked to the provision of services, there is a clear expectation that partner organisations will maintain at least the same levels and approaches to information security as the Trust.

1.4 Responsibility for information security resides, ultimately, with The Trust's Chief Executive, Executive Directors or equivalent responsible officers where these responsibilities have been formally delegated. This responsibility will be discharged through a designated member of staff who has lead responsibility for information security management within the organisation. The information security lead (SIRO) is of appropriate seniority and is an Executive Director that is a member of the Trust Board with voting rights. Equally the Caldicott Guardian is of equal seniority but also has a clinical lead within the Trust. These lead roles are formally acknowledged and will be made widely known throughout the organisation through this policy and other communications.

2 Purpose

2.1. Objectives

The objectives of Lincolnshire Partnership NHS Foundation Trust Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2. **Policy aim**

The aim of this policy is to establish and maintain the management, security and confidentiality of information, information systems, applications and networks owned or held by Lincolnshire Partnership NHS Foundation Trust by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principless of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.
- Ensuring that those with a specific responsibility for information management understand what is required and are trained appropriately.

2.3. **Scope**

This policy applies to all information, information systems, networks, applications, locations and users of Lincolnshire Partnership NHS Foundation Trust or supplied under contract to it and workers as part of their duties when employed or acting on behalf of the Trust.

3 Duties

3.1. Ultimate responsibility for information security rests with the Chief Executive of Lincolnshire Partnership NHS Foundation, but on a day-to-day basis the Senior Information Risk Officer (SIRO) shall be responsible for managing and implementing the policy and related procedures.

3.2. Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters
- Are up to date with an acceptable level of information governance training based on their role

3.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

3.4. Information Asset Owners who are responsible for systems and data ensure that those systems and data are secure, managed effectively and in line with legislation and that an audit of security, access controls and information and data flows is carried out at least annually. In addition that there is a business continuity plan for all critical systems that they have responsibility for.

3.5. The Information Security Policy shall be maintained, reviewed and updated by the IM&T Committee. This review shall take place at least annually.

3.6. Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

3.7. Each member of staff is responsible for ensuring they maintain their level of knowledge and training, to allow them to meet the requirements of their role in respect of information management and security.

3.8. Each member of staff shall be responsible for the operational security of the information systems they use and the information they input into it.

3.9. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard. This includes the accuracy, timeliness and availability of data and information they are responsible for. They will also comply with the agreed operating guidelines/policies for each system at all times.

3.10. Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

3.11. Where possible, and in addition, contractors/suppliers will have completed an information governance review to a recognised national standard to offer further assurance to the organisation of the robustness of their systems and processes.

3.12. Failure to comply with part or all of these responsibilities, either wilfully or through neglect, may lead to disciplinary action where appropriate or in the case of contractors, termination of their contract.

4 Definitions

Lincolnshire Partnership NHS Foundation Trust shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their NHS information assets.

4.1 The classification **NHS Confidential** – shall be used for patients' clinical records, patient identifiable clinical information passing between NHS staff and between NHS staff and staff of other appropriate agencies. In order to safeguard confidentiality:

- The term "NHS Confidential" shall **not** be used on correspondence to a patient in accordance with the Confidentiality: NHS Code of Practice.
- Documents so marked shall be held securely at all times in a locked room to which only authorised persons have access.
- They shall not be left unattended at any time in any place where unauthorised persons might gain access to them.
- They should be transported securely in sealed packaging or locked containers. Users breaching these requirements may be subject to disciplinary action.

4.2 The classification **NHS Restricted -** shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or it's officers or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

NHS Restricted documents should also be stored in lockable cabinets

5 Legislation

5.1. Lincolnshire Partnership NHS Foundation Trust is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Lincolnshire Partnership NHS Foundation Trust, who may be held personally accountable for any breaches of information security for which they may be held responsible. The Trust shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001

5.2 The Trust shall also maintain its annual registration with the Information Commissioner.

6 Policy Framework

6.1. Management of Security

- At board level, responsibility for Information Security shall reside with the nominated director leads (SIRO and Caldicott Guardian)
- The Trust's Information Governance specialist and its Information Security Lead shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation
- The Deputy Director of Performance and Information shall have overall responsibility for ensuring the operational implementation of this policy
- Information and systems leads will have delegated responsibilities in respect of their roles.

6.2. Information Security Awareness Training (mandated)

- Information security awareness training shall be included in the staff induction process (to include records management and information governance).
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

6.3. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause that details each member of staff's responsibilities in respect of information security.
- Information security expectations of staff with specific responsibilities shall be included within job definitions.

6.4. Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian (Information Asset Owner) who shall be responsible for the information security of that asset, its management and its disposal (where authorised by the SIRO). The existing custodian remains responsible for updating the asset register where the circumstances have changed in relation to the asset. This includes where the asset is no longer serviceable, has been passed to a new user, or is to be returned into stock to be reallocated. All assets remain the property of the Trust and not individual workers or managers.

6.5. Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

6.6. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

6.7. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have a business need to use the facilities. Where this access is abused or circumstances change this facility may be removed permanently or temporarily at the discretion of the SIRO.

6.8. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

6.9. **Equipment Security**

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Where possible this will include protecting equipment through password protection and encryption in line with national guidelines and in accordance with Trust policy on e-mail, mobile working and the computer use.

6.10. **Computer and Network Procedures**

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the IM&T Committee.

6.11. **Information Risk Assessment**

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the Trust's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

6.12. **Information security events and weaknesses**

All information security events and suspected weaknesses are to be reported through the incident management in accordance with the Trust's risk management incident policy arrangements. All information security events shall be appropriately investigated to establish their cause and impacts with a view to avoiding similar events.

6.13. **Classification of Sensitive Information.**

(see section 4)

6.14. **Protection from Malicious Software**

The organisation shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy. **Users shall not install software on the organisation's property without permission from the SIRO or delegated officer. Users breaching this requirement may be subject to disciplinary action.**

6.15. **User media**

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Trust's IM&T lead before they may be used on Lincolnshire Partnership NHS Foundation Trust systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action and have their access rights removed.

6.16. **Monitoring System Access and Use**

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures

- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

6.17. **Accreditation of Information Systems**
The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the SIRO and Caldicott Guardian before they commence operation and that a privacy impact assessment has been completed.

6.18. **System Change Control**
Changes to information systems, applications or networks shall be reviewed and approved by the SIRO on the advice of the Information Security Manager.

6.19. **Intellectual Property Rights**
The organisation shall ensure that all information products are properly licensed and that they are approved by the SIRO on the advice of the Information Security Manager. Users shall not install software on the organisation's property without permission from the Head of ICT. Users breaching this requirement may be subject to disciplinary action.

6.20. **Business Continuity and Disaster Recovery Plans**
The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks. Sections on procedural action in the event of the loss of computer, software or systems access will be included in all operational service business continuity and disaster recovery plans.

6.21. **Reporting**
The Information Security Officer shall keep the IM&T Committee informed of the information security status of the organisation by means of regular reports and presentations. The ICT services lead will also provide the organisation with regular reports on reported issues through the helpdesk, network availability and downtime, system and network security assurance and planned developments.

6.22. **Policy Audit**
This policy shall be subject to audit by the Trust's internal auditors and annual Information Governance Toolkit Assessment.

6.23. **Further Information**
Further information and advice on this policy can be obtained from the Deputy Director of Performance and Information, Trust HQ.

6.24 **Review and revision arrangements**
This policy will be reviewed at least annually by the author and in line with Trust policy on the review of policies.

6.25 **Dissemination and Implementation**
This policy will be disseminated utilising the Trust's current arrangements. The policy will also be disseminated through the IM&T Committee members. Implementation will be through training at induction, Records Management Training and Systems Training. There will also be awareness raising, through computer logon screens and references made in associated policies and guidance.

6.26 **Policy Control including Archiving Arrangements**

Policy control and archiving will be carried out in accordance with the Trust's current arrangements.

6.27 **Monitoring Compliance**

The Trust will monitor compliance with this policy through regular audit and review and through monitoring the number and type of incidents related to information security.

7. Audit and Monitoring

Systems	**Monitoring and/or Audit**				
Criteria	Measurables	Lead Officer/Group	Frequency	Reporting to	Action Plan/ Monitoring
Application of Procedures	Internal Audit programme	Deputy Director of Performance and Information	Annually	Audit and Assurance	IM&T Committee
	Incident reporting	Information Governance Group	Monthly	IM&T Committee	Information Governance Group
	Induction Training	Training Department	As and when required	IM&T Committee	Information Governance Group
	Mandatory IG Training	Training Department	Annual	Board of Directors	Workforce Committee
	Audit of information and data flows	Information Asset Owners	Annual	IM&T Committee	Information Governance Group

8. Policy approved by:

Signature _____ Date 2012

Chris Slavin
Chief Executive
Lincolnshire Partnership NHS Foundation Trust

9. References

1. Connecting for Health Information Governance Toolkit V10 2012

10. Appendices

Lincolnshire Partnership NHS
NHS Foundation Trust

GENERIC EQUALITY IMPACT ASSESSMENT TEMPLATE

INITIAL EQUALITY IMPACT ASSESSMENT

STAGE 1 - Screening to establish if the proposed function has any relevance to any equality issue and/or minority group			
Directorate: **Strategy, Performance & Information**	**Function to be Assessed: Information Management & Security Policy**	**Existing or New Function: Existing**	**Assessment Date: 22/07/2012**
1. Briefly describe the aims, objectives and purpose of the function:	Providing an Information security management framework to preserve confidentiality, integrity and availability of information across all information system, networks and users of LPFT		
2. Who is intended to benefit from this function, and in what way?	Staff, management, service users and carers and partner agencies by setting standards for security of information		
3. What outcomes are wanted from this function?	Staff compliance with relevant legislation. Understanding of the principles of information security and how these will be implemented ensuring a consistent approach to security creating an awareness of the need for information security and protecting information assets.		
4. What factors/forces could/ contribute/ detract from these outcomes?	Lack of training for staff. Failure of staff to implement standards. Lack of resources.		
5. Who are the main stakeholders in relation to the function?	Executive team and Board of Directors. Information Governance and IM&T Committee, system users and line managers.		
6. Who implements the function, and who is responsible?	Everyone working in the NHS has responsibilities to adhere to the standards in this policy. Chief Executive has ultimate responsibility, Director of Finance and Compliance has Trust Board level accountability. Head of Information Governance has day to day responsibility		
7. Are there concerns that the function has a differential impact on the following groups and what existing evidence (either presumed or otherwise) do you have for this? No Impact			

8. If concerns about the policy in terms of differential impact are echoed by the views of experts or relevant groups, then a Full EIA must be undertaken. Should the function proceed to a full EIA? no

If no, please state date of next review: October 2013
If yes, please state the date on which full impact assessment to be completed by:

I understand the Impact assessment of this function is a statutory obligation and that, as owners of this function, we take responsibility for the completion and quality of this process.

Signed (Completing Officer).....Date.....November 2012.....

Print Name:.....Steve Lidbetter, Deputy Director of Performance & Information.....

Signed (Section Head)..... Date.....

Print Name:.....Jane Marshall, Director of Strategy, Performance & Information.....

Please note: This Impact Assessment will be scrutinised by the Equality and Diversity Group, and moderated by the WOD Committee

APPENDIX

Lincolnshire Partnership NHS
NHS Foundation Trust

Information Governance Management Framework

2012

1. Contents

Item No.	Contents	Page No.
1.	Contents	2
2.	Document History	2
3.	Introduction and Purpose	2
4.	Scope	2
5.	IG Roles & Responsibilities	3
6.	Resources	3
7.	IG Policies & Procedures	3
8.	Internal IG Governance (Bodies & Structure)	4
9.	Training & Guidance	4
10	IG Awareness	5
11.	IG Reporting	5
12.	Caldicott Function	5
13.	IG Toolkit and independent auditing	5

2. Document History

Task/Action	Lead	Approvals	Date
Final Draft for sign-off	Steve Lidbetter	IM&T Committee	27th November 2012
Dissemination of framework	Steve Lidbetter/Communications Department	IM&T Committee	27th November 2012

3. Introduction & Purpose

The Information Governance Framework brings together related initiatives concerned with improving the security, processing, quality and handling of information. It Incorporates the Data Protection Act 1998, the Freedom of Information Act 2000, the Human Rights Act 1998 and the common law duty of confidence. It also incorporates the NHS Code of Confidentiality; Information Security Assurance, Information Quality Assurance and Records Management and underpins the NHS Care Record Guarantee.

4. Scope

The IG Framework is the control assurance framework which is formed by those elements of law and policy from which applicable Information Governance standards are derived. It applies only to internal Information Governance assurance.

5. IG Roles & Responsibilities

IG Function	Job Title
SIRO and Information Governance Director Lead	Director of Strategy Performance and Information
Deputy SIRO	Deputy Director of Performance and Information
Caldicott Guardian	Medical Director
Information Governance Work stream Lead	Deputy Director of Performance and Information
Confidentiality Lead	Caldicott Guardian
DPA and Registration Authority	Head of Information Governance (Shared Service)
Information Security	Information Security Manager (Shared Service)
Freedom of Information	Trust Secretaries Office

6. Resources

The Director Lead for Iinformation Governance (SIRO) will hold the budget for internal IG as part of their role as budget holder for Lincolnshire Partnership NHS Foundation Trust and will be responsible for highlighting any resourcing issues and improvements required either in year or for the forthcoming year.

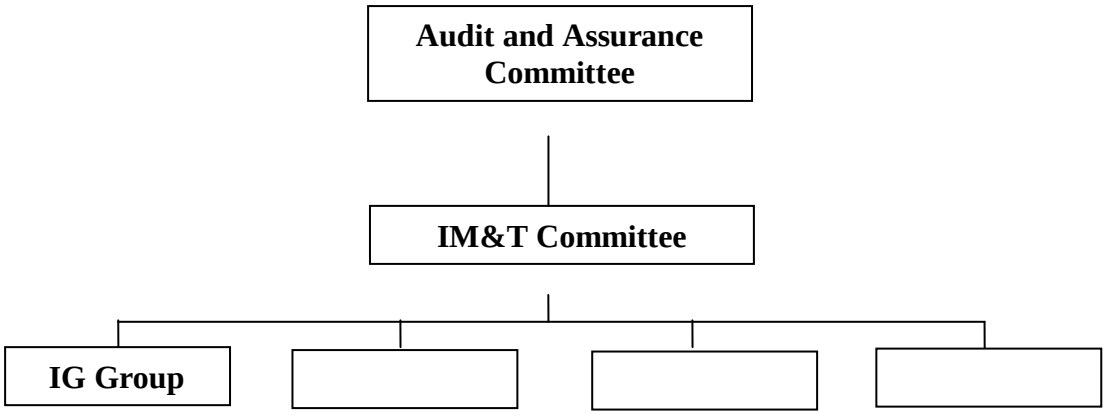
7. IG Policies & Procedures

Policy Name	Review Date	Approval Body	Review Body
Records Management and Lifecycle Policy	Annual	IM&T Committee	Records Management Group
Information Security Policy	Annual	IM&T Committee	IG Group
Computer and Technology Policy	Annual	IM&T Committee	IM&T Committee

All policies will be disseminated/cascaded via Lincolnshire Partnership NHS Foundation Trust Communication Team. Lincolnshire Partnership NHS Foundation Trust Lead will attend the IM&T Committee in order to brief respective leads to ensure a robust cascade of information.

To obtain assurance that implementation of policies and the development of robust information governance is subject to effective planning, Lincolnshire Partnership NHS Foundation Trust Lead will utilise and review, audit and incident findings, that are IG related and report these to the IM&T Committee through the Information Governance Group update report. This information will also form part of the awareness campaign for IG with serious incidents forming part of the IG Group and IM&T Committee Risk Register.

8. Internal IG Governance (Bodies & Structure)



9. Training & Guidance

Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. The following approach ensures that all staff receives training appropriate to their roles:

- All staff will be briefed on IG requirements as part of their induction.
- Complete an accredited annual refresher.
- Receive face to face training if required.
- Complete additional IG training based on the requirements of their role.

10. IG Awareness

To ensure that raising awareness of a compliance with information governance standards is raised. Lincolnshire Partnership NHS Foundation Trust will utilise the NHS Confidential IG Campaign developed by NHS East Midlands and deployed regionally.

To ensure that this campaign has been implemented and all staff have been informed of their responsibilities a staff survey will be undertaken post and prior to delivery of the internal campaign.

In addition it will continue to raise awareness about national and local incidents that re quire cascading by doing this through identified communication routes.

11. IG Internal Reporting

Lincolnshire Partnership NHS Foundation Trust Board of Directors receive periodic assurance that management and accountability arrangements are adequate and are informed in a timely manner of future changes in the IG agenda by IG updates within the IM&T Committee report.

The IG Work stream will also:

- Report IG incidents to the IG Group
- Analyse, investigate and upward report of incidents and any recommendations for remedial action
- Produce IG work programme progress reports
- Report on annual IG assessment and improvement plans
- Communicate IG developments and standards to appropriate forum and staff

Policy and procedures for actual and potential breaches of confidential and person identifiable information are aligned with the guidance provided within the 'Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents' – Gateway ref: 13177

12. Caldicott Function

Lincolnshire Partnership NHS Foundation Trust must have in place a recognised senior level Caldicott guardian. The Caldicott functions will be maintained by the Caldicott guardian.

The Caldicott functions will also be maintained by the Caldicott guardian by exception with the support of the Information Governance Group and Information Governance Work stream

Lead. Any issues, incidents and strategy relating to this function will be incorporated within overarching internal Information Governance arrangements.

13. IG Toolkit and independent auditing

The Trust will complete the requirements of the self-assessment against the standards in the IG Toolkit and submit them periodically as required. The Trust will also undergo an annual independent audit of its IG arrangements and its clinical coding arrangements and processes. The findings will form part of the overall IG and Caldicott Guardian work plan.

In addition the Trust will complete audits of its systems and processes at least on an annual basis including:

- Review of data flow mapping.
- Review of its network and server security
- Review of its critical information systems management and access controls

14. Review of this Framework

These arrangements and the framework document will be reviewed at least annually.