NHS
Vale of York
Clinical Commissioning Group

Item 11

Information Governance Strategy

Information Governance Strategy :	VOY xx
Date Issued:	
Date To Be Reviewed:	Annually

Policy Title:	Information Governance Strategy	
Supersedes:	All previous Information Governance Strategies	
Description of Amendments	18/12/13: Initial draft 19/12/13: Update to reporting structure	
This policy will impact on:	All Vale of York Clinical Commissioning Group staff	
Financial Implications:	No Change	
Policy Area:	Information Governance	
Version No:	1.2	
Issued By:		
Author(s):	Barry Jackson, Information Governance, Security & Compliance Manager, North Yorkshire and Humber CSU/Pennie Furneaux Policy & Compliance Manager	
Document Reference:		
Effective Date:		
Review Date:		
Impact Assessment date:		
APPROVAL RECORD		
Consultation:	Vale of York Clinical Commissioning Group Information Governance Steering Group	
	North Yorkshire and Humber Commissioning Support Unit IG Team	
Committees:		

Contents

Introduction and Purpose

The purpose of this strategy is to describe the management arrangements that will deliver Information Governance assurance within the Vale of York Clinical Commissioning Group.

Information Governance provides a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information, allowing:

- implementation of central advice and guidance;
- compliance with the law;
- year on year improvement plans.

Information Governance is about setting a high standard for the handling of information and giving organisations the tools to achieve that standard. The ultimate aim is to demonstrate that an organisation can be trusted to maintain the confidentiality and security of personal information, by helping individuals to practice good information governance and to be consistent in the way they handle personal and corporate information.

The Information Governance Toolkit (IGT) is an online tool that enables organisations to measure their performance against the information governance requirements and compliance with the toolkit provides assurance that organisations have established good practice around the handling of information, are actively promoting a culture of awareness and improvement to comply with legislation and other mandatory standards.

National Context

The NHS Information Governance Assurance Programme (IGAP) was established in February 2008 in response to the Cabinet Office Data Handling review. The Prime Minister commissioned the review following the high-profile data losses in 2007. IGAP developed a number of principles to support and strengthen the existing Information Governance agenda.
The principles are:

- All NHS organisations should be part of the same Information Governance Assurance Framework
- Information Governance should be as much as possible integrated into the broader governance of an organisation, and regarded as being as important as financial and clinical governance in organisational culture
- The Framework will provide assurance to the several audiences interested in the safe custody and use of sensitive personal information in healthcare. This involves greater transparency in organisational business processes around Information Governance
- IGAF to be built on the strong foundations of the existing Information Governance agenda and is the mechanism by which:
    - IG policies and standards are set
    - Regulators can check an organisation's compliance
    - An organisation can be performance managed

Aim

The purpose of this local framework is to set out an overall strategy and promote a culture of good practice around the processing of information and use of information systems. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The organisation requires all employees to comply with the Policies, Procedures and Guidelines which are in place to implement this framework with the aim of ensuring that the Vale of York Clinical Commissioning Group maintains a high quality IG service.

Information Governance is linked to the organisation's Assurance Framework, reference 5; the potential Risk that the CCG may lack capability and capacity to deliver strategic priorities and legal responsibilities. Specific Information Governance objectives are detailed at Annex A

Information Governance Toolkit

Completion of the IGT is mandatory for all organisations connected to N3, using NHS Mail and providing NHS services. All organisations are required to score on all requirements at level 2 or 3 to be at a satisfactory level. Annual plans will be developed year on year from the IGT to achieve a satisfactory level in all requirements. As the IGT is a publically available assessment the scores of partner organisations will be used to assess their suitability to share information and to conduct business with.

The Information Governance Statement of Compliance

The Information Governance Statement of Compliance, (IGSoC) is the process by which organisations enter into agreement with HCIC for access to its services. The terms and conditions of access are set out in the IG Assurance Statement which is a required element of the IG Toolkit. It is essential that every organisation meets the obligations of the IG Toolkit, and complies with the IG Assurance Statement to the required standards to safeguard HSCIC services and information for all.

The IG Assurance Statement includes:

- the requirement that no Patient Identifiable Data or other sensitive data be stored or processed offshore where the location is deemed non-compliant with the HSCIC Offshore Policy;
- the right to audit by HSCIC or nominated third parties;
- Change Control Notification procedures and approvals processes; and
- the requirements for reporting security events and incidents.

North Yorkshire & Humber Commissioning Support Unit (NYHCSU)

The Vale of York Clinical Commissioning Group has in place an SLA agreement with NYHCSU to deliver a range of IG services including delivery of the IG Toolkit at Level 2. The full NYHCSU IG Framework is set out at Annex B and describes how the organisation is set up to provide these services to its customers.

This strategy should be viewed in conjunction with the North Yorkshire & Humber Commissioning Support Unit Information Governance Framework detailed at Annex B.

Duties and Responsibilities

Vale of York Clinical Commissioning Group Governing Body

The Clinical Commissioning group Governing Body is responsible for defining policy in respect of Information Governance, taking into account the statutory and NHS mandatory requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to deliver the Information Governance Agenda.

The Chief Clinical Officer

The Chief Clinical Officer has overall responsibility for Information Governance and is the Accountable Officer. The Chief Clinical Officer is required to sign off the Information Governance Statement of Compliance, (IGSoC) before the final annual submission of the Information Governance Toolkit.

Caldicott Guardian

The Caldicott Guardian for the Vale of York Clinical Commissioning Group is the Chief Nurse.

The Caldicott Guardian is responsible to act as a champion for data confidentiality and to develop a knowledge of confidentiality and data protection matters including links with external sources of advice and guidance. They should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff and oversee all arrangements, protocols and procedures where confidential information may be shared with external bodies including disclosures to other public sector agencies and other outside interests.

Senior Information Risk Owner

The SIRO for the Vale of York Clinical Commissioning Group is the Chief Operating Officer.

The SIRO is responsible for leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers. Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs and advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls.

Managers

Managers are responsible for ensuring that their staff, both permanent and temporary, are aware of:

- all information security policies and guidance and their responsibility to comply with them;
- their personal responsibilities for information security;

- where to access advice on matters relating to security and confidentiality; and
- the security of their physical environments where information is processed or stored.

Staff

Individual employees have a responsibility to ensure they are aware of all information security policies and guidance and comply with them. Staff must be aware of their personal responsibility for the security and confidentiality of information which they use. Staff are responsible for reporting any possible or potential issues whereby a breach of security may occur.

Information Security

With the increasing use of electronic data and ways of working which rely on the use of electronic information and communication systems to deliver services there is a need for professional advice and guidance on their use as well as the need to ensure that they are maintained and operated to the required standards in a safe and secure environment.

Data Protection Act

The Data Protection Act is the most fundamental piece of legislation that underpins Information Governance. Vale of York Clinical Commissioning Group are registered with the Information Commissioners Office and will fully comply with all legal requirements of the Act. A process will be adopted to ensure that a review of all of new systems is carried out and where requirements such as the need for Privacy Impact Assessments are highlighted these will be completed.

Risk Management

The ability to apply good risk management principles to IG is fundamental and all organisations will apply them through organisational policies. The NYHCSU IG Team will be responsible for completion of the risk assessments for any IG related issue, and have a specific remit to risk assess new technologies and recommend controls where necessary.

Training and Guidance

In accordance with the requirement to achieve Level 2 on the IG Toolkit all staff must complete an Induction session when they first start employment which will include Information Governance. In subsequent years all staff are required to complete further Information Governance training as set out in the on line IG Training Tool. Within the IGTT there are specific modules available for Caldicott, SIRO and IG staff themselves. Appropriate staff must complete the modules relevant to their roles. The way in which all staff will access this training is through the IG Training Tool: http://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm
Staff awareness of IG will also be assessed by questions in the annual staff survey in order to provide assurance that the training is sufficient.

The CCG will implement an approved Information Governance Training Matrix that details the training appropriate for each staff group.

Awareness and Advice

The NYHCSU IG Team will provide advice on any IG related issue. They will be responsible for the production of newsletters and all staff e-mails to provide information to staff on IG issues.

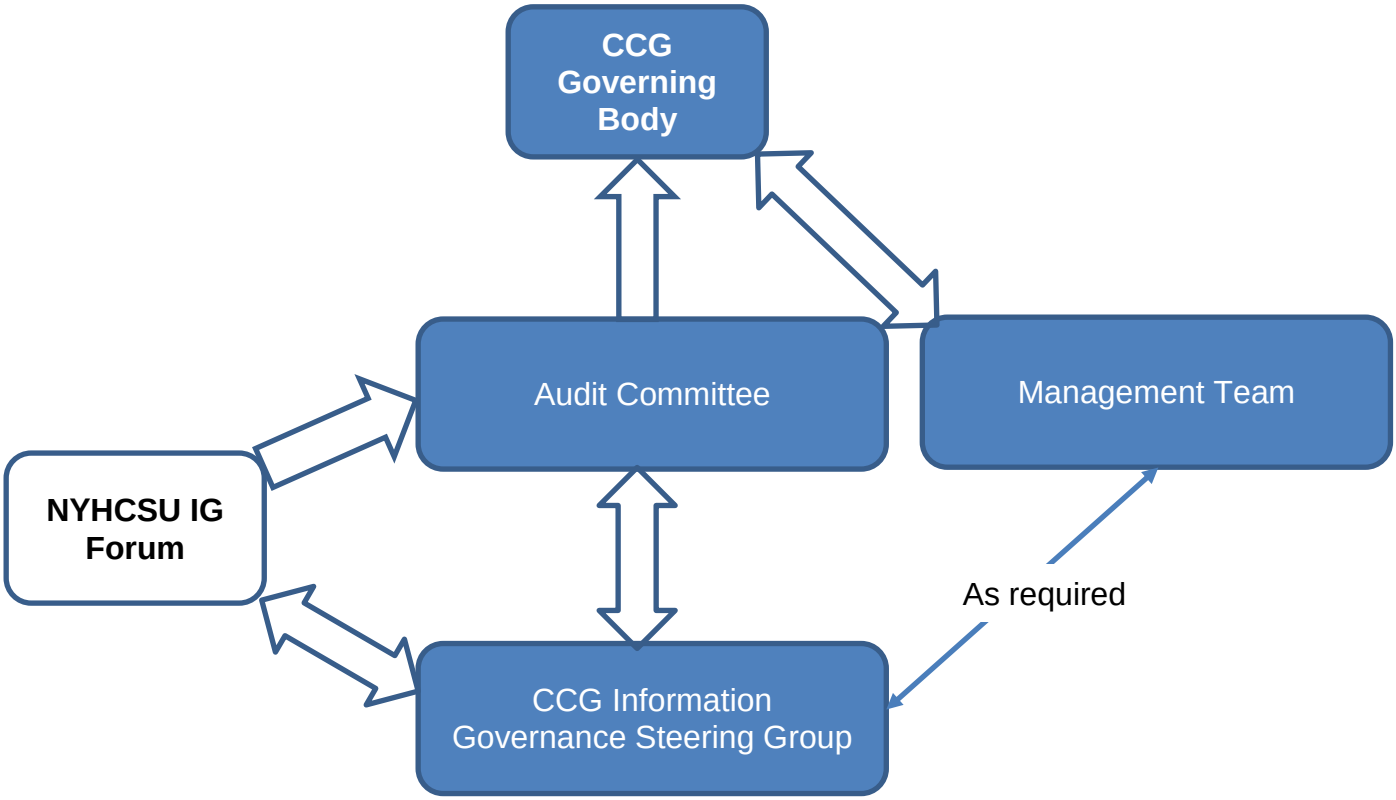
Incident Management

Incidents must be reported and managed through the local incident management process. The NYHCSU IG Team will have an active involvement in all IG related incidents and IG related service desk calls to ensure compliance with IG principles. Significant issues will be subject to full investigation and reporting action. Incidents relating to personal information will be highlighted to the Caldicott Guardian whilst those of a more technical nature will be reported to the SIRO.

Investigation

The NYHCSU IG Team will be responsible for the investigation of all IG issues reported. This may include but is not limited to, breaches of policy, breaches of confidentiality and issues related to IT Security. The Information Governance & Security Manager is a police trained investigator and the IG Team will maintain the procedural processes to ensure that investigations of incidents will be carried out in a way that ensures the preservation of evidence and in a manner that enables both legal and disciplinary action to be taken if necessary.

Organisational Structures



CCG Information Governance Steering Group

The organisation has implemented an Information Governance Steering Group that reports to the Audit Committee. The Information Governance Steering Group will be the organisation's forum with delegated authority to oversee Information Governance issues, assurance and work plans.

Key Policies and Procedures

The organisation will implement a number of Information Governance Policies which will be published on the organisation's intranet and internet sites. Key policies relate to:

- Overarching Information Governance Policy
- Confidentiality and Data Protection;
- Information security and risk;
- Information lifecycle management including records management and information quality; and
- Corporate governance including Freedom of Information

In addition the organisation will implement a number of supporting standards and procedures which also be published and made accessible to staff.

ANNEX A

CCG Strategic Objectives: Link to the CCG Assurance Framework

Ref. 5.1 Potential Risk: Lack of CCG capability and capacity to deliver strategic priorities and legal responsibilities

Objective		Assurance Provided By:
1	To establish a robust information governance framework that conforms to Department of Health standards that provides appropriate assurance regarding the efficient, effective, secure and legal processing of all information.	Annual review and sign off of an organisational Information Governance Strategy
2	Maintain a clear outline of responsibilities and reporting structure for all information governance functions.	Implementation of the organisation's and operation of the approved Information Governance Strategy.
3	To ensure that the Governing Body is appraised of the Information Governance agenda, receives periodic assurance that management and accountability arrangements are adequate and assurance that the CCG is fulfilling their obligations.	Annual report to the Governing Body and ad hoc reporting during the year as required.
4	To use the Information Governance Toolkit as the driver for the main Information Governance work programme reflecting the business needs of the CCG and any other national requirements such as Informatics Planning, or special directives issued by the Department of Health.	Adherence to the Information Governance Toolkit reporting and submission agenda Completion
5	To ensure that there is a suite of policies that encompasses all the elements of information processing that comply with legal and ethical requirements and best practice.	Implementation of Information Governance Policies and related Standards
6	To ensure that there are clearly defined processes in place to support the policies.	CSU Information Governance Forum and Vale of York CCG Information Governance Steering Group
7	To ensure that organisational information systems, procedures and working practices conform to Information Governance standards	Implementation of Information Governance Policies and related Standards
8	To ensure that clear advice and guidance is available for staff and to ensure that they understand and apply Information Governance in their daily working practice	Publication of up to date Information Governance documentation on the organisation's intranet

Objective		Assurance Provided By:
9	To ensure that measures are in place to ensure that information is of the highest possible quality.	SLA and reports from the CSU Business Intelligence Unit
10	To undertake regular reviews and audits on the various aspects of information processing. To ensure that such reviews and audits are used to identify good practice and opportunities for improvement.	Outcomes of Internal Audit Information Governance and other related reviews.
11	To ensure that all policies and procedures are monitored and reviewed regularly to ensure that they are adhered to and are effective.	Outcomes from the programme of reviews and monitoring arrangements agreed with the CSU.
12	To ensure that all staff, service users and the general public will have confidence in the way that we process their information.	Publication of a Fair Processing Notice. Up to date Guidance published on the organisation's web site.
13	To ensure that clear advice is given to all data subjects about how their personal information is processed, and to ensure that there is a mechanism to deal with all enquiries.	
14	To ensure that when service developments or modifications are undertaken, that a review is undertaken of all aspects of information governance arrangements to ensure that they are robust and effective.	Privacy Impact Assessment guidance and procedure published on the intranet
15	To continuously improve the information governance culture across the CCG through training and awareness campaigns.	Approved Information Governance work plan.
16	To ensure that there is a comprehensive proactive information risk management programme.	Report of outcomes of Information Risk Assessments to the SIRO
17	To ensure that all information governance incidents or near misses are notified, investigated and actioned appropriately in accordance with HSCIC IG Toolkit requirement 349 and CCG policies and procedures.	Report of information governance incidents, complaints and audits are monitored by the Information Governance Steering Group
18	To strive for year-on-year improvements in compliance with the Information Governance Toolkit standards across the CCG.	CCG Information Governance work plan.
19	To ensure that independent contractors comply with Information Governance principles.	Use of approved Information Governance clauses in contracts
20	To support the commitments of the NHS Care Record Guarantee.	Information Governance Toolkit performance and compliance to Level 2.

ANNEX B

The North Yorkshire & Humber CSU Information Governance Framework

Information Governance Framework (V1.1 dated 19th February 2013)

Introduction and Purpose

The purpose of this framework is to describe the management arrangements that will deliver Information Governance assurance within North Yorkshire & Humber CSU as well as to all its customers. Information Governance is a framework that enables the organisation to establish good practice around the handling of information, promote a culture of awareness and improvement and comply with legislation and other mandatory standards.

National Context

The NHS Information Governance Assurance Programme (IGAP) was established in February 2008 in response to the Cabinet Office Data Handling review. The Prime Minister commissioned the review following the high-profile data losses in 2007. IGAP developed a number of principles to support and strengthen the existing Information Governance agenda.
The principles are:

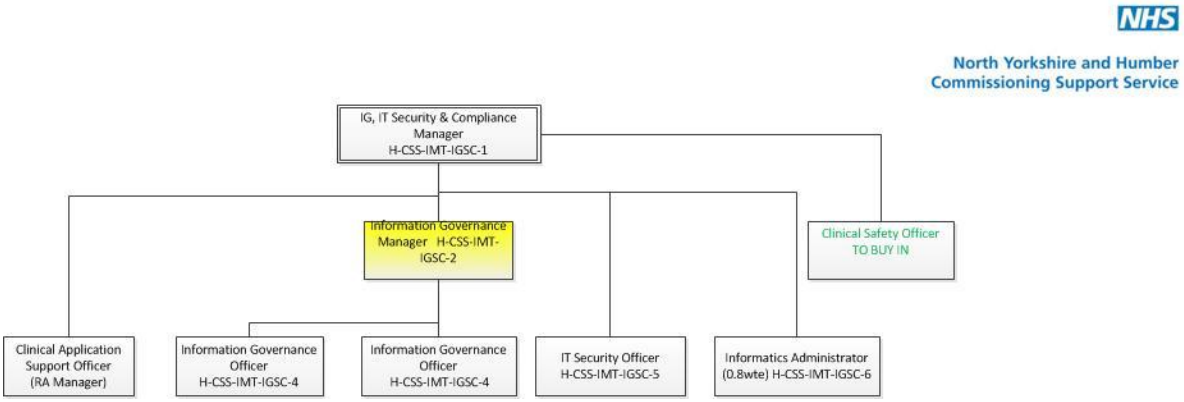
- All NHS organisations should be part of the same Information Governance Assurance Framework
- Information Governance should be as much as possible integrated into the broader governance of an organisation, and regarded as being as important as financial and clinical governance in organisational culture
- The Framework will provide assurance to the several audiences interested in the safe custody and use of sensitive personal information in healthcare. This involves greater transparency in organisational business processes around Information Governance
- IGAF to be built on the strong foundations of the existing Information Governance agenda and is the mechanism by which:
    - IG policies and standards are set
    - Regulators can check an organisation's compliance
    - An organisation can be performance managed

Aim

The purpose of this local framework is to set out and promote a culture of good practice around the processing of information and use of information systems that supports the provision of high quality care to users of our services. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The organisation requires all employees to comply with the Policies, Procedures and Guidelines which are in place to implement this framework with the aim of ensuring that the CSU delivers a high quality IG service both internally and to all its customers.

Information Governance Security & Compliance Team.

The structure of the team is shown here. It will be hosted within the IMT Department and consists of staff based at locations across the whole CSU area. .



Information Governance Toolkit

Completion of the IGT is mandatory for all organisations connected to N3, using NHS Mail and providing NHS services. All organisations are required to score on all requirements at level 2 or 3 to be at a satisfactory level. Annual plans will be developed year on year from the IGT to achieve a satisfactory level in all requirements. In addition to the NYHCSU assessment the IG Team will work with customers to ensure that they achieve satisfactory levels. As the IGT is a publically available assessment the scores of partner organisations will be used to assess their suitability to share information and to business with.

Caldicott Guardian

The Caldicott Guardian for NYH CSU will be the Strategic Nurse and Head of Clinical Quality and Assurance.

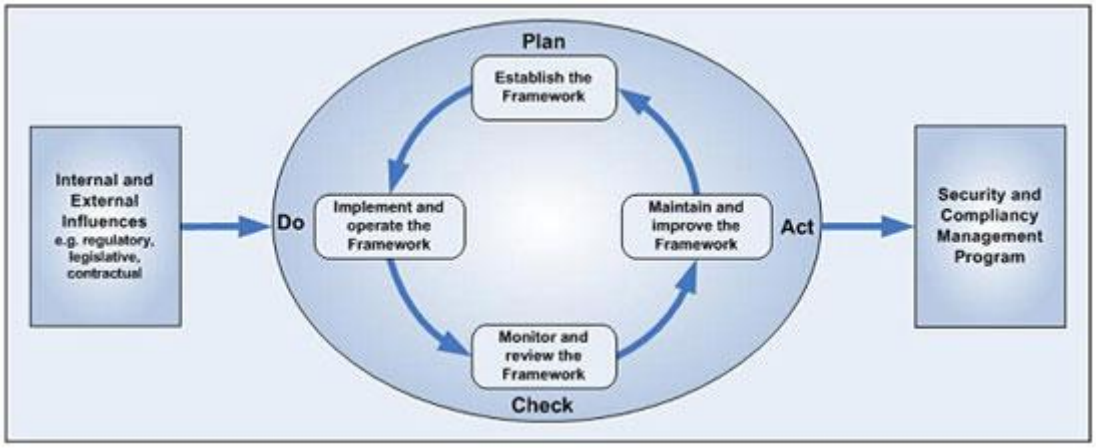
The Caldicott Guardian is responsible to act as a champion for data confidentiality and to develop a knowledge of confidentiality and data protection matters including links with external sources of advice and guidance. They should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff and oversee all arrangements, protocols and procedures where confidential information may be shared with external bodies including disclosures to other public sector agencies and other outside interests.

Information Security

With the increasing use of electronic data and ways of working which rely on the use of electronic information and communication systems to deliver services there is a need for professional advice and guidance on their use as well as the need to ensure that they are maintained and operated to the required standards in a safe and secure environment.

ISO 27001

The IG Team will work toward the nationally recognised standard Information Security Management System as described in ISO27001. The standard formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organisations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard which will be a significant advantage in a commercial environment. The standard is based around the principles of Plan, Do, Check, Act.



Support to Projects

Based in the IMT Department the IG Team will ensure that the best principles of IG are incorporated into all projects by being fully engaged in all aspects of project and programme management. They will ensure that projects have a formal IG stage and approval as well as providing continual advice and assistance as required.

Data Protection Act

The Data Protection Act is the most fundamental piece of legislation that underpins Information Governance. The IG Team are all formally training in its operation and are able to provide advice on its implementation by staff across a range of work areas. This will specifically include guidance to new project and around the introduction of new systems where requirements such as the need for Privacy Impact Assessments will become the norm.

Risk Management

The ability to apply good risk management principles to IG is fundamental and all organisations will apply them through organisational policies. The IG Team will be responsible for completion of the risk assessments for any IG related issue, and have a specific remit to risk asses new technologies and recommend controls where necessary.

Senior Information Risk Owner

The SIRO for NYH CSU will be the Business Services Director.

The SIRO is responsible for leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers. Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs and advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls.

Training and Guidance

In accordance with the requirement to achieve Level 2 on the IG Toolkit all staff must complete an Induction session when they first start employment which will include Information Governance. In subsequent years all staff are required to complete further Information Governance training as set out in the on line IG Training Tool. Within the IGTT there are specific modules available for Caldicott, SIRO and IG staff themselves. Appropriate staff must complete the modules relevant to their roles. The way in which all staff will access this training is through the IG Training Tool: http://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm
Staff awareness of IG will also be assessed by questions in the annual staff survey in order to provide assurance that the training is sufficient.

Awareness and Advice

The IG Team will provide advice on any IG related issue. They will be responsible for the production of newsletters and all staff e-mails to provide information to staff on IG issues.

Registration Authority

The IG Team will be responsible for the management, policy and strategic delivery of the Registration Authority (RA) function. The RA function is defined by national policy and relies on a series of overlapping systems including confirmation of identity to the recognised standard of e-Gif Level 3, the issue of a chip and pin smartcard containing digital certificates, and a system of complex access rights, business functions and activities within the User Identity Management system to enforce Role Based Access Control to sensitive information.

Incident Management

Incidents must be reported and managed through the local incident management process. Occasionally incidents are reported in the first place to the Informatics Service Desk. The Information Governance team will manage all IG related incidents and IG related service desk calls to ensure compliance with IG principles. Significant issues will be subject to full investigation and reporting action. Incidents relating to personal information will be highlighted to the Caldicott Guardian whilst those of a more technical nature will be reported to the SIRO.

Investigation

The Information Governance Team will be responsible for the investigation of all IG issues reported. This may include but is not limited to, breaches of policy, breaches of confidentiality and issues related to IT Security. The Information Governance & Security Manager is a police trained investigator and the IG Team will maintain the procedural processes to ensure that investigations of incidents will be carried out in a

way that ensures the preservation of evidence and in a manner that enables both legal and disciplinary action to be taken if necessary.

Clinical Safety Officer

The role of Clinical Safety Officer is to maximise the benefits of patient safety from new technology and, at the same time, minimise any risks that the new technology itself could introduce so that NHS IT systems can support clinicians in providing better, safer patient care. The responsibility for this role sits within the IG Team structure but it is expected that when such expertise is required it will be sought from external organisations.

Support to Customers

The IG Team will provide a range of support to any customer of the CSU based on the details set out in the IMT service specification. The primary role for the team however will be the delivery of the IG Toolkit at level 2 to the 8 CCGs. This delivery is based on the process shown here: