South Tees Hospitals NHS
NHS Foundation Trust

Agenda Item 10.1

Meeting / committee:	Board of Directors	**Meeting date:**	27th August 2013

Title:	Information Governance Annual Report 2012/13 & 2013/14 Strategy

Purpose:	This report is to inform the Board of Directors of progress against the Information Governance (IG) work programme in 2012/13 and to outline the key priorities and associated work programmes for 2013/14.

Key issues / items for consideration in the report:	The Board is advised that: • A significant amount of progress has been achieved over the past year • The structure of the information governance (IG) team has been reviewed and changed to ensure that it continues to meet the needs of the organisation whilst at the same time supporting the directorate cost improvement programme • The IG service is joining the Quality & Assurance Directorate with effect from 1st September 2013 • The work programme for this year aims to meet the priorities of the trust but continues to need organisational support if the targets are to be achieved

Prepared by:	Nicky Huntley Head of Information Governance	**Presented by:**	Joanne Dewar Director of IT & Health Records Nicky Huntley Head of Information Governance

Recommendation:	The Board of Directors is asked: • to note the progress made in 2012/13 • approve the High Level Project Plan (appendix B) • note the IG Toolkit baseline score for July's required submission. (appendix C)

Implications (please mark an X)	Legal	Financial	Safety & Quality	Strategic	Risk & Assurance
	X	X	X	X	X

South Tees Hospitals NHS Foundation Trust
Information Governance Annual Report 2012/13 & Strategy for 2013/14

1. Executive Summary

1.1 The purpose of this report is to confirm the Trust's progress within the Information Governance Assurance Framework for 2012/13 and to set out the key areas of work for 2013/14. To aid the reader's understanding, a glossary is attached at Appendix A.

1.2 Information governance ensures necessary safeguards for, and appropriate use of, patient and personal information. The Information Governance (IG) Framework, which is currently managed by the Health & Social Care Information Centre, brings together all the requirements, standards and best practice that apply to the handling of personal information to ensure:

- Compliance with the law
- Implementation of Department of Health advice and guidance
- Planned year on year improvement

1.3 All public and private organisations are legally obliged to protect any personal information they hold and public authorities are also obliged to provide public access to official information.

1.4 The Information Commissioners Office (ICO) is the UK's independent public body set up to protect personal information and to promote public access to official information.

1.5 Section 2 and 3 of the report adds further understanding of the background of information governance and how the framework is devolved within the organisation.

1.6 Section 4 highlights the progress against the IG framework for 2012/13. In summary the trust has:

- submitted a score of 74% (Green Satisfactory) on the IG Toolkit
- declared itself SoC Compliant (statement of compliance) by achieving a minimum level 2 on all IG Toolkit standards
- received Full Assurance for the first time in the annual IG audit report
- strengthened the information risk management framework across the Trust with divisional IG Leads
- continued to show a year on year decline in the number of reportable IG incidents
- successfully transferred SystmOne Units from the PCT over to South Tees
- achieved 91.45% staff compliance on IG annual mandatory training (over 21% increase on 2011/12)
- introduced Train the Trainer allowing divisional staff to develop skills and deliver IG training within their own areas.

1.7 To ensure an adequately resourced and skilled IG compliance unit, a full review of the IG department took place in August 2012, reducing staff expenditure which contributed to the directorate's cost improvement programme.

1.8 Section 5 introduces the information key drivers and work plans for 2013/14, setting out the strategy to further strengthen the Trust's IG compliance, including:

- IG department to transfer to Quality & Assurance Directorate from 1st September 2013
- work to achieve level 3 on all IG Toolkit standards
- review, consider and implement recommendations where possible from the recent Information Governance Review (Caldicott2)
- keep abreast of pending data protection changes in Europe and UK.
- review, consider and implement the new IG incident reporting framework
- further standardise the process for patient/staff access to their personal information.

- review the Protection of Freedoms Act 2012 and advise on compliance requirements.
- advise on the development of the Trust's Publication Scheme
- supporting divisional and directorate wide data protection audits

1.9 Appendix B provides the IG high level Project Plan for 2013/14 in more detail, including key actions and timescales.

1.10 Section 6 highlights key risks to achievement of the work plan, summarised below:
.

- continued support from all trust staff to complete annual mandatory IG training
- IG involvement in a number of the work streams for the Transforming the Care we Deliver programme
- consistent approach across the trust with the management of information requests and archived information
- the need for a trust wide integrated system for recording subject access requests and other related divisional information for IG compliance.
- the work to complete data protection audits by divisions and directorates in preparation for the pending ICO powers to audit NHS organisations.
- proposed changes to EU and UK data protection legislation

1.11 Section 7 offers a summary of the report confirming that last year has again seen an increase in demand on trust resources dedicated to the IG programme. The team has worked hard to ensure that the trust has kept up with the pace of the demands of the national information governance agenda, in addition to the day to day operational aspects of IG.

2. Background

2.1 Information governance (IG) is the way by which an organisation handles all of its information, in particular its personal and sensitive information. It allows organisations and individuals to ensure that personal information is dealt with legally, securely, ethically and efficiently in order to deliver the best possible care.

2.2 Information governance provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of information and has four fundamental aims:

i) To support the provision of high quality care by promoting the effective and appropriate use of information.

ii) To encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.

iii) To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.

iv) To enable organisations to understand their own performance and manage improvement in a systematic and effective way.

2.3 A full review of the IG department was undertaken in August 2012. In order to ensure an adequately resourced and skilled IG compliance unit the following changes were introduced:

- Remove 1 x Band 6 wte post from the structure.
- Appoint 1 x Band 4 wte Information Governance Assistant – Training.
- Consider the current scope and remit of the IG work and prioritise appropriately to enable the service to be facilitated within reduced resource levels.
- Deliver an IG structure which will:

- Provide appropriate IG polices and processes which comply with all appropriate national and local IG standards.
- Provide and monitor required IG training via appropriate methods of delivery.
- Provide practical support and guidance to senior managers with responsibility for IG related areas of work.
- Provide leadership and support to ensure organisational understanding and adherence to IG policy across the workforce.
- Inform the organisation on its compliance across the IG agenda.

2.4 The Information Governance Department currently consists of the following:

- Head of Information Governance
- Deputy Information Governance Manager
- IG Specialist – Information Rights Management & Compliance
- IG Specialist – Security & Compliance
- IG Assistant x 2
- Admin support

2.5 In June 2010 the trust appointed Professor Rob Wilson as Caldicott Guardian. The Caldicott Guardian is a senior person within an organisation who is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

2.6 The trust currently has an Information Governance Steering Group to provide advice and assurance to the trust on all matters concerning information governance. The group is chaired by the Director of IT & Health Records as the Senior Information Risk Owner (SIRO) and authorised by Formal Management Group to fulfil its duties and make recommendations within its terms of reference.

2.7 Each division/directorate is required to have a representative at the IG Leads Forum. This group has recently replaced the Data Quality and Information Governance Forum as the operational group which reports to and from the Information Governance Steering Group. The group consists of representatives from each division/directorate.

2.8 Each representative is responsible for information governance and able to actively support the implementation of IG initiatives across the trust including evidence of information governance compliance to support the IG Toolkit annual self-assessment. The forum deals with operational issues and concerns regarding data quality and information governance and acts as a vehicle for training and awareness sessions for representatives to feedback within their divisions/directorates. The IG Leads Forum reports to the Information Governance Steering Group.

3. Legislation, National Standards & Policy

3.1. Legal & Professional Obligations

3.1.1 There is a range of complex legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly a range of statutes that permit or require information to be used or disclosed. The Department of Health has now produced ***NHS Information Governance – guidance on legal and professional obligations***, a best practice guidance document which outlines the likely impact of these provisions primarily on NHS information, but it also includes some social care information. The requirements of the Freedom of Information Act 2000, Data Protection Act 1998 and Human Rights Act 1998 (Article 8 – privacy) are incorporated into the IG Framework.

3.1.2 Presently the most commonly dependent legislation, guidance and national standards around Information Governance are:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Computer Misuse Act 1990
- IG Toolkit
- NHS Information Governance Statement of Compliance
- NHS Information Risk Management
- International Standard for Information Security: ISO/IEC 27002:2005
- Health & Social Care Information Centre
- Care Quality Commission
- NHS Operating Framework
- NHS Quality Accounts
- NHS Code of Practice: Confidentiality
- NHS Code of Practice: Records Management
- NHS Code of Practice: Information Security Management

3.2 Information Commissioner's Office - Data Protection Notification Changes

3.2.1 The Information Commissioners Office (ICO) maintains a public register of data controllers (Notification). Each register entry includes the name and address of the data controller and a general description of the processing of personal information by a data controller. A data controller must inform the ICO of any changes as soon as possible and in any event within 28 days. Failure to keep a register entry up to date is a criminal offence. No new Notifications were made for the trust in 2012/13.

3.3 Information Commissioner's Office –Powers

3.3.1 As a data controller the trust has a legal obligation under the Data Protection Act 1998 to protect and keep secure all of the personal and sensitive information it comes in to contact with in the course of providing its services to the public.

3.3.2 Security issues and data breaches are always high profile and the IG Department has been involved in informal complaints around breaches/potential breaches of confidentiality. Therefore it is vital that staff adhere to the policies and procedures that have been developed to ensure that adequate safeguards are in place for the processing of personal data.

3.4 Information Governance Assurance Statement of Compliance (SoC)

3.4.1 The Information Governance Assurance Statement of Compliance (SoC) is the agreement between NHS Connecting for Health (CfH) and Approved Service Recipients. It sets out the information governance policy and terms and conditions for use of NHS Connecting for Health services.

3.4.2 The SoC contains a number of obligations to enable use of NHS CfH's services, which aim to preserve the integrity of these services. It is essential that every organisation meets its statement obligations to the required standards to safeguard NHS CfH's services and information for all. The trust currently uses a number of these services such as the Choose and Book system for appointments and referrals, and the Summary Care Record for the validation of patient demographics.

3.4.3 To achieve SoC the organisation has to achieve Level 2 or above on the requirements of the IG Toolkit. Where the minimum IG Toolkit standards are not met an action plan for making the necessary improvements must be agreed with the Department of Health Information Governance Policy Team (via the Strategic Health Authority for 2012/13).
The trust declared itself SoC compliant in 2012/13 as the trust had met all standards at minimum level 2 or above.

3.5 Monitor

3.5.1 Monitor's Compliance Framework for 2012/13[1] confirms that NHS foundation trusts are required to meet the relevant requirements of the Information Governance Toolkit, as set out by the Department of Health.

3.5.2 Monitor considers a robust information governance assurance framework to be a fundamental component of good governance. However, they regard the achievement of these specific requirements as a contractual matter for foundation trusts and their commissioners. As is Monitor's general practice, where another agency takes the regulatory lead, in this case, the Information Commissioner, Monitor will not generally take action unless and until other bodies have exhausted their powers and the foundation trust still risks breaching its Authorisation.

3.5.3 The trust declared itself SoC compliant in 2012/13 as the trust had met all standards at minimum level 2 or above.

3.6 Policies

3.6.1 There is consistent scrutiny, government reports and recommendations around information governance, in particular around data handling. Policies and procedures can be found easily via the trust's intranet site and are updated accordingly to reflect any new guidance or change in practice etc.

3.6.2 An IG policy plan is in place for the on-going management of current and newly identified policies and Standard Operating Procedures (SOPs) ensuring that these are reviewed and updated as necessary.

3.7 Information Governance Reviews & Consultations

3.7.1 Caldicott2 -The Information Governance Review[2]

3.7.1.1The NHS Future Forum Work stream on information noted a number of issues regarding the perception of information governance in particular with regards to sharing information, even when this is in the best interest of the patient. In its report the Forum recommended that:

> …*The Government should commission a review of the current information governance rules and of their application, to report in 2012. The aim of the review should be to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care*[3]…

3.7.1.2 In January 2012, the Government accepted this recommendation, and the then Secretary of State for Health asked Dame Fiona Caldicott to lead a new independent review of information governance across the whole health and social care system in England. In order to distinguish this review from Dame Fiona's report in 1997, it became known as the Caldicott2 review.

3.7.1.3 The report was published in March 2013 with a total of 26 high level recommendations. The Secretary of State for Health should maintain an oversight of these recommendations and is requested to publish an assessment of the implementation of the recommendations within a 12 month period of the publication of the final report.

3.8 Ministry of Justice (MoJ): Assessment Notices under the Data Protection Act 1998 Extension of the Information Commissioner's Powers

[1] Monitor Compliance Framework 2012/2013

[2] Caldicott2 - The Information governance Review

[3] Information: A Report from the NHS Future Forum, January 2012

3.8.1 The Information Commissioner has requested that the Secretary of State use the Order-making power under section 41A (2)(b) Data Protection Act (DPA) to extend the powers of the Information Commissioner to carry out compulsory assessments of NHS bodies' compliance with the data protection principles under the DPA.

3.8.2 On the 25th March the MoJ launched the above consultation[4] aimed at NHS data controllers in England, Wales and Northern Ireland bodies and Health Service data controllers in Scotland.

3.8.3 A summary of the consultation and a draft response on behalf of South Tees NHS Foundation Trust was provided to Corporate Directors in May 2013. The response was agreed and submitted to the MoJ by the Head of Information Governance. The consultation closed on 27th May 2013 with a response due to be published within three months.

3.9 EU Data Protection Reform – Summary so far

3.9.1 In 2009 the European Commission (EC) launched its first public consultation with a view to revising the European Data Protection Framework. After much debate and consideration the UK Government responded to the UK Justice Select Committee's report on the EU data protection reform. Currently numerous EU member states have contributed to over 300 proposed amendments which are presently under consideration. In a statement[5] the Information Commissioner announced that..

…put simply, the proposals could prove to be one of the biggest changes to data protection this country has ever seen….

The ICO are currently monitoring events in Europe closely, looking at how initial reform proposals might be brought into UK law.

4. <u>Information Governance Progress 2012/13</u>

4.1 Audit & Monitoring – Information Governance Toolkit Assessment & Results

4.1.1. NHS organisations are mandated to submit, via Connecting for Health, an annual self-assessment of their information governance status. This is achieved via the Information Governance Toolkit (IG Toolkit). The IG Toolkit is used to measure progress against key requirements. The 2012/13 IG Toolkit scores were required to be submitted thrice yearly:

- 31 July 2012 - Benchmark submission
- 31 October 2012 - Baseline submission
- 31 March 2013 - Final submission

4.1.2 The IG Toolkit uses a framework of standards, which are designed to ensure organisational compliance with statutory and mandatory requirements concerning the management of patient, staff and corporate information. The IG Toolkit has been developed as the principal mechanism by which IG policy can be broken down into measurable components in order to assess an organisation's performance annually through a system of self-assessment and audit. The IG Toolkit enables the organisation to develop a strategy and annual work programme to raise the level of compliance year-on-year, and also improve its information risk management process.

4.1.3 The IG Toolkit assessment score is used to inform the National Information Governance Board and the Care Quality Commission. NHS Quality Accounts now include IG assurance within their performance assessments. A requirement for internal

[4] https://consult.justice.gov.uk/digital-communications/ico-assessment-notices/consult_view

[5] http://www.ico.org.uk/news/blog/2013/eu-data-protection-reforms-how-the-process-works-and-what-the-ICO-is-doing

audit of IG has been formally established by including IG performance in NHS organisations' statement of Internal Control and Annual Report.

4.1.4 The Information Governance Toolkit currently encompasses the following:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information assurance
- Secondary Use Assurance
- Corporate Information Assurance

4.1.5 Connecting for Health review the requirements of the Information Governance Toolkit annually to ensure the following functional aspects:

- to provide interpretive advice and guidance
- to provide a means of self assessing performance against key aspects of information governance
- to support the independent assurance of information governance returns

4.1.6 The IG Toolkit End of Year Report 2012/13 was submitted as a position statement of 75% to the Integrated Governance Committee at it's meeting on the 13th March 2013. The final score was confirmed at 74% and was submitted by the Trust at the end of March 2013. The scores provided by the Trust are required to be internally and externally verified. This is currently done:

- Internally - The Trust's Financial Services Manager prior to final submission.
- Externally – The Trusts Internal Auditors, Audit North provide a sample review of standards within the Toolkit prior to final submission. The auditors produced a report which concluded in full assurance with no recommendations.

4.1.7 The IG Toolkit levels of scoring are based on a two tier Red (unsatisfactory) or Green (satisfactory) system of reporting. Connecting for Health has classified that having one standard "red unsatisfactory" will impact on the overall status of the toolkit as "red unsatisfactory", thus giving a false reflection of an organisations overall general IG performance. Table 1 below highlights the IG toolkit scores across the region.

Table 1

PUBLISHED TOOLKIT SCORES 31st MARCH 2013 (VERSION 10) Acute Hospitals	**%**	**RAG**
SOUTH TYNESIDE FOUNDATION NHS TRUST	81	Satisfactory
CITY HOSPITALS SUNDERLAND NHS FOUNDATION TRUST	84	Satisfactory
GATESHEAD HEALTH NHS FOUNDATION TRUST	87	Satisfactory
THE NEWCASTLE UPON TYNE HOSPITALS NHS FOUNDATION TRUST	82	Satisfactory
NORTHUMBRIA HEALTHCARE NHS FOUNDATION TRUST	92	Satisfactory
SOUTH TEES HOSPITALS NHS TRUST	74	Satisfactory
NORTH TEES AND HARTLEPOOL NHS FOUNDATION TRUST	81	Satisfactory
COUNTY DURHAM AND DARLINGTON NHS FOUNDATION TRUST	87	Satisfactory

4.1.8 All responsible requirement owners' collated electronic evidence in the secure section of the allusers fileshare and a detailed work programme was kept up to date by the Information Governance team and monitored by the Information Governance Steering Group (IGSG) on a bi- monthly basis.

4.1.9 2012/13 saw v10 IG Toolkit Work Programme integrated into the trusts Health Assure system, and updated to evidence compliance.

4.1.10 Table 2 highlights the separate GP IG Toolkit score for the Marske Medical Centre and the Resolution Centre. Discussions have taken place around the possibility of a single inclusive IG toolkit for submission which will reflect the organisation as a whole. However at the moment this forms part of the governance requirements of the GP contract and so will remain as is until further notice.

Table 2

GP IG Toolkit v10 completion	Overall Score	Grade
Marske Medical Centre	79%	Satisfactory
Resolution Centre	79%	Satisfactory

4.1.11 The information governance team, along with the divisional/directorate IG Leads have worked hard to ensure full compliance with the IG Toolkit for 2012/13 and as a result all standards scored a minimum of a level 2 Green (satisfactory) prior to 31st March 2013. The achievements this year resulted in the trust receiving a "Full Assurance" for the first time in its annual IG Internal audit report.

4.2 Confidentiality and Data Protection Assurance

This area of work specifically addresses**:**

- NHS Code of Practice: Confidentiality
- Data Protection Act 1998

4.2.1 Incident Management

4.2.1.1 The trust must publish details of any personal information related incidents categorised as Serious Untoward Incidents (level 3-5) as part of the Statement of Internal Control and Annual Report.

4.2.1.2 Between April 2012 and March 2013, there was one serious untoward incident of the severity rating 3. This incident was reported to the Information Commissioner and several pieces of information were requested by the ICO so that they could evaluate the trust's investigation and response to the loss. The ICO's decision was that the incident did not meet the criteria set out in their Data Protection Regulatory Action Policy necessitating further action by the ICO. This decision was due to the particular facts of the case and the remedial measures set out by the trust. In addition the trust had been able to evidence that all personnel involved were up to date with their information governance training.

4.2.1.3 Personal data related incidents classified at a severity rating of levels 1 and 2 are summarised in the required Department of Health format below.

Table 3

Summary of Personal Data Related Incidents In 2012/13 **LEVEL 1-2 ONLY**		
Category	**Nature of Incident**	**Total**
I	Loss of inadequately protected electronic equipment, devices or paper documents from secured NHS premises	2
II	Loss of inadequately protected equipment, devices or paper documents from outside NHS premises	0
III	Insecure disposal of inadequately protected electronic equipment, devices or paper documents	0
IV	Unauthorised disclosure	0
V	Other	0

4.2.1.4 For the incidents above, the trust is confident that the missing information has not been in the public domain.

4.2.1.5 The trust continues to show a year on year decline in the number of Serious Untoward IG incidents for all levels 1 to 5

Table 4

09-10	10-11	11-12	12-13
9	6	5	3

4.2.2 Standardisation of Data Protection Processes

4.2.2.1 Under the Data Protection Act (DPA) 1998 organisations have a statutory duty to respond to requests for personal information within a time period of 40 calendar days. However although DPA states 40 days to comply, a government commitment requires that for health records, requests should normally be handled within 21 days.

4.2.2.2 The review of the trust's data protection processes for the handling of subject access requests has now been completed and a DPA Subject Access Request Implementation Plan is in place incorporating the health records manager, Trust solicitor and facilitated by the head of information governance.

4.2.2.3 The plan highlights 3 phases, phase 1 seeing a new framework for handling requests across the trust being implemented including the transition of current staff and resources. Phase 2 requires a review of systems and administration processes to reflect the new framework and subsequent transitions and phase 3 will see a campaign across the trust, raising awareness to staff and patients on their information rights and processes to gain access to their information in line with legislation. June 2013 saw the completion of phase 1.

4.2.2.4 Throughout the year, the IG team has seen a significant increase in the involvement of complex subject access requests. These pose a significant strain on the department with regard to compliance with timescales and resourcing the work.

4.2.3 Information Sharing

4.2.3.1 Information Sharing Agreements (ISA's) have been developed for either providing or taking part in services or situations that require information to be shared as part of that agreement. Agreements signed up to, or reviewed, are detailed below in table 5.

Table 5

Title	Owner	Purpose	Status
Cleveland Local Resilience Forum	Lead by Tees PCT – now NECSU	To support information sharing with local agencies that are responsible for emergency planning and response.	Complete
Combined Hospices Information Sharing Agreement	South Tees NHS Foundation Trust	An agreement currently exists with Teesside Hospice to support the provision of seamless care to cancer patients. This agreement is to be widened to encompass other Hospices where required. The Butterwick Hospice is now to be included.	Currently underway.
Multi Agency Overarching Information Sharing Protocol	Joint Ownership between South Tees, County Durham and	This protocol sets out the legal basis when considering the sharing of personal information. It is intended to act as an agreement between signatories showing	The trust has signed the reviewed protocol. The document is

(v7 Review)	Darlington and North Tees NHS Foundation Trusts. This Protocol currently covers organisations within County Durham & Darlington, Tees Valley and North Yorkshire Area	that they are aware of the requirements and confirm their intention to commit to information sharing where there is a legitimate need. It is expected that signatories meet the minimum responsibilities as set out within the protocol	fluid and due to the NHS organisational changes further signatories will be added.

4.3 Information Security & Information Risk Management Assurance

4.3.1 Information Security

4.3.1.1 The trust's deputy information governance manager oversees a fortnightly Formal Trust IT Security Meeting attended by IG Specialist: Security & Compliance, the ICT Communications Manager and the ICT Infrastructure Security Analyst. This group ensures that the trust can constantly review emerging threats and issues and provides expert guidance and action in relation to the information security agenda. The group also contribute to ad-hoc discussions regarding current on-going web shop reviews and various local / regional security issues. Issues and actions are noted, monitored and escalated where appropriate.

4.3.1.2 A number of information security reviews have been completed over the course of the year, the most significant being:

- Transforming the Care We Deliver –
  - Data Centre Reviews
  - Help Desk Reviews
- Cloud Security Reviews
  - Hospital case management programme Medworxx
  - Mobile Device Management Solution
- Forensic analysis of Trust equipment as part of various internal investigations.

4.3.1.3 All information security reviews have followed the trust Information Risk Management Framework procedure of being provided to the SIRO for review and approval and where appropriate an accompanying Caldicott Approval Form has been completed by the external company and approved by the trust Caldicott Guardian.

4.3.1.4 As in previous years, the information governance team has encouraged the use of the national Information Governance Training Tool, which has proven to be extremely useful in providing training and guidance to all levels of staff across the trust. It utilises information security guidance videos and slides to provide advice and knowledge appropriate to various staff roles.

4.3.2 Information Risk Management and the establishment of IG Leads

4.3.2.1 The trust has previously adopted and implemented the national Information Risk Management framework using a structured approach. The trust assigned the "ownership" of information assets to senior accountable staff. Divisional managers and corporate directors were designated as Information Asset Owners (IAO's) and operational staff, with day to day responsibility for managing risks to their information assets, identified as Information Asset Administrators (IAA).

4.3.2.2 Information Governance Leads have been established within all divisions and these key staff (all of whom are IAA's) are now responsible for raising awareness of IG issues within their own directorates. This may include being trained by the IG team to deliver training out to various staff within their own division. The IG Leads are also responsible for completion of an action plan to ensure that the evidence required by the IG Toolkit

2012/13 which relates to divisional information is provided in a timely manner. On the whole this has proved to be a very successful approach to ensure that information risk has successfully been devolved within the trust.

4.3.3 E-Safety – Safeguarding in a Digital World

4.3.3.1 The Local Safeguarding Children Board (LSCB) has an expectation that the trust develops an environment where children, young people and adults who work with them can use the Internet and other digital technologies safely and securely.

4.3.3.2 South Tees NHS Foundation Trust takes seriously the role it has to ensure that it co-operates to safeguard and promote the welfare of children and young people in the locality, and to ensure that the trust is effective in doing so. The head of information governance is currently the trust E-safety Lead and is working in partnership with the Safeguarding Team to ensure that awareness training forms part of the trusts Safeguarding Children training. This ensures that staff are aware of their responsibilities to e-safety and safeguarding children in a digital world.

4.3.3.3 As part of promoting the welfare of children and young people in accordance with the Children Act 2004 and Working together to safeguard children 2006, the LSCB has devised an e-safety strategy plus a policy that is built on four key areas:

1. Policies, practices and procedures
2. Education and training
3. Infrastructure and technology
4. Standards and inspection.

4.3.3.4 The trust currently has an E-safety Action Plan in place, monitored by the Information Governance Steering Group. This action plan will contribute to the LSCB Section 11 compliance audits (M*ulti-agency safeguarding children information to assist good practice*). Due to clinical staffing changes there are actions that still need completing, however these will be picked up as part of the High Level IG Work Programme for 2013/14.

4.4 Corporate Information Assurance

This area of work specifically addresses**:**

- Freedom of Information Act 2000
- NHS Code of Practice: Records Management

4.4.1 Freedom of Information

4.4.1.1 The Freedom of Information Act (FoIA) came into force at the beginning of 2005. It deals with access to official information, while parallel regulations deal with environmental information. The Act provides individuals or organisations with the right to request information held by a public authority. They can do this by letter or email. The public authority must tell the applicant whether it holds the information and if so, must supply it within 20 working days, in the format requested (unless exemptions apply). The Act is fully retrospective and applies to all information, not just information filed since the Act came into force. Compliance with the Act is overseen by the Information Commissioner's Office which is the UK's independent authority set up to promote access to official information and to protect personal information.

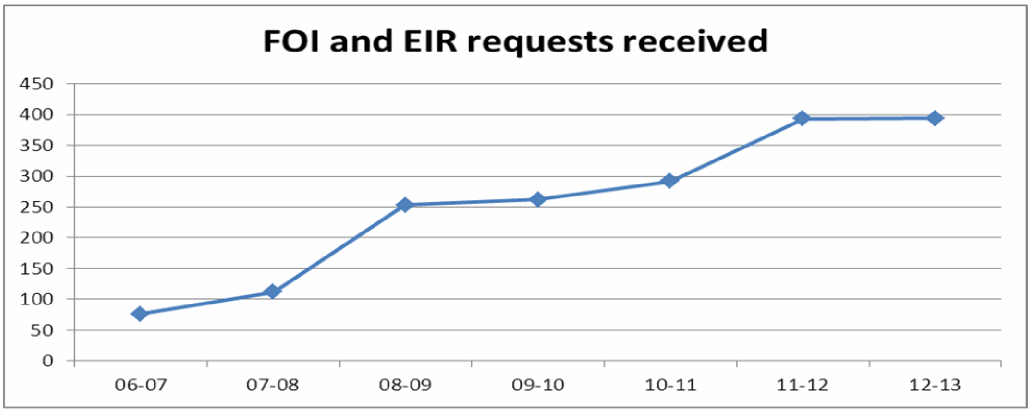
4.4.1.2 The Environmental Information Regulations (EIR) 2004 only provide public access to environmental information held by public authorities whilst the Freedom of Information Act gives people access to most other types of information held by public authorities.

4.4.1.3 All responses to a FoIA or EIR request now include a customer satisfaction survey. Out of all the requests received in the last financial year only 12 surveys were returned. However the responses received were very encouraging.

Table 6	Very good	Good	Satisfactory	Poor
Quality of service provided	9	3		
Timely acknowledgement of request	10	1	1	
The degree to which the response answered your request	9	2	1	
Ease of understanding of the response	10	1		
Overall helpfulness of the response	10	2		
Additional comments	Great service, thanks for your help South Tees Trust has been outstanding in its response to all of my FoIA requests so far			

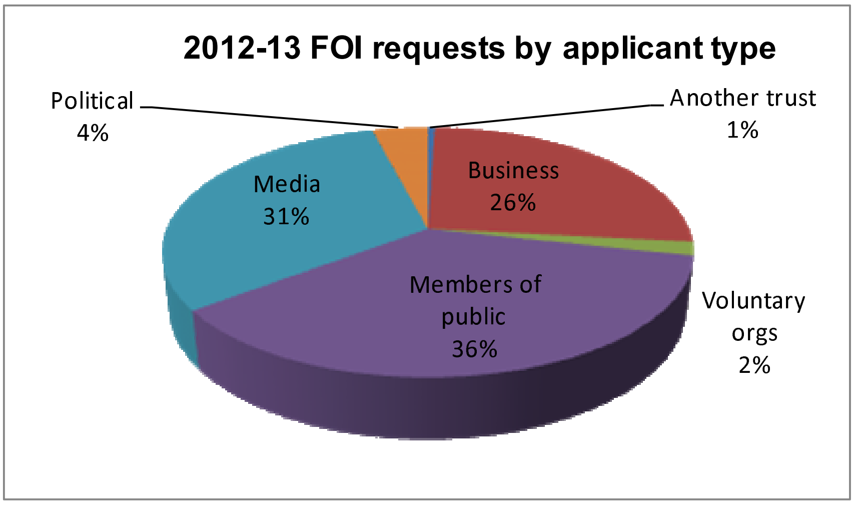
4.4.1.4 The trust has received 394 FoIA requests for the year 2012-2013. This is the first time that there has been no or very little increase in the number of requests since the introduction of the Freedom of Information Act in 2005.

Table 7



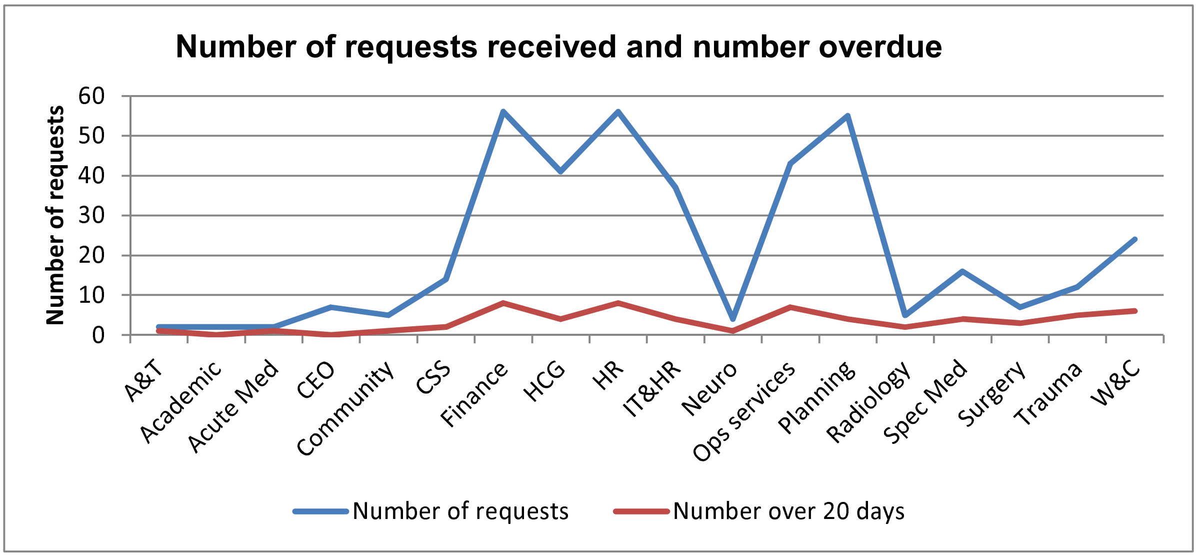
4.4.1.5 For the year 2012/13, compliance with the 20 day time limit for response was 84%, this is an improvement of 3% on the previous year but still under the compliance rate of 85% (the ICO state less than 85% will be a trigger for investigation). The number of requests where the trust has used an exemption has decreased considerably since the last quarter of 2011/12 with only 5% of requests over the year subject to an exemption.

Table 8



4.4.1.6 The type of applicant submitting FoIA requests has remained fairly static over the past 2 years and members of the public still appear to be the largest category. However it is well recognised that many requests are submitted by the media or businesses using staff member's personal email addresses to disguise their real identity. This has no effect at all on the processing of the request as the same information is released regardless of the origin of the request.

Table 9



4.4.1.7 It is a requirement of the Freedom of Information Act 2000 that every public authority must adopt and maintain a publication scheme. A publication scheme is a commitment to routinely and proactively provide information to the public. In 2011 the ICO confirmed that renewed guidance concerning what needed to be included in a Publication Scheme would be released, however to date, this guidance has yet to be published.

4.4.1.8 The trust's website has recently been reviewed by the CEO's office and all out of date information removed. There will be further communication between CEO's office and newly appointed divisional web editors, to ensure that the required information is published onto the trust internet site and kept up to date, thus ensuring a current trust Publication Scheme.

4.5 Connecting for Health (CfH) & the National Programme for IT (NPfIT)

4.5.1 Registration Authority (RA)

4.5.1.1 The NHS Care Records Service Registration Authority is responsible for registering and verifying the identity of NHS staff that need to use the NHS Care Records Service and related IT systems and services, including SystmOne, Summary Care Record, Choose and Book, and the Electronic Staff Record.

4.5.1.2 Access to these computer systems and services is controlled by smartcards which are similar to a chip and pin credit card, verified by a unique passcode. Registration authorities issue smartcards to staff after an e-GIF level 3 identity check has been completed and organisational sponsorship provided. This is essential to protect the security and confidentiality of every patient's personal and healthcare information.

4.5.1.3 The management of Smartcard maintenance, including unlocking and renewing, has been delegated across the organisation. This includes the set-up of RA Workstations across divisions/locations to ensure staff are able to easily amend their Smartcard when necessary. The RA Manager will audit all activity on any workstations that are set up to ensure consistency and secure smartcard management is upheld across the organisation.

4.5.1.4 The trust recently took over the management of RA for community staff who transferred from Tees PCT. The RA function for community staff in North Yorkshire & York is currently managed via a service level agreement.

4.5.1.5 In January 2013 an audit of RA was carried out and produced 5 key recommendations. An action plan is in place and monitored by the ESR User Group:

- The trust must complete Integrated Identity Management across the whole of the organisation
- Smartcard related software must be upgraded to the most recent version on all machines – enabling functions such as self-service
- RA resources must be reviewed
- The trust's new starter form must include indication of smartcard requirements
- The RA provisions outlined in the service level agreement should be reviewed to ensure a robust service.

4.5.2 Integrated Identity Management

4.5.2.1 It is important that everyone who will have access to patient information has been through the same rigorous identity checks. Integrated Identity Management allows these checks to be done once, at the stage of employment, rather than repeated a second / third time during employment. The integration of the RA system (UIM) and the Payroll system (ESR) means that the level of access to patient information an individual will have, will be decided by the position they hold in the organisation.

4.5.2.2 Integrated Identity Management addresses three key areas: HR / RA integration, Position Based Access Control (PBAC) and the UIM/ESR interface. The trust is now live with the UIM/ ESR interface and the RA Manager and Payroll team have so far successfully allocated over half of all smartcard users with a specifically allocated PBACs agreed by the organisation. This control ensures that levels of access are determined by the ESR position meaning that no one member of staff has more or less access than they require to carry out their job role. Recruitment staff are now logging ID checks into ESR meaning that duplication of ID checking for elements such as smartcards has been removed.

4.5.2.3 The RA project team has successfully implemented the first stage of Integrated Identity Management and is now focused on assigning PBAC to all of the community staff. The smartcard profiles existing in community are more complex due to the nature of access to SystmOne.

4.5.3 Summary Care Record Implementation into Secondary Care

4.5.3.1 The Summary Care Record (SCR) application is currently used amongst clerical staff to obtain patient demographics, NHS numbers and GP details. The full Summary Care Record allows clinicians to access information such as any medication the patient is on / has been on and any allergies or adverse reactions the patient has. Both levels are accessed through the secure National Spine Portal using minimum search criteria of gender, surname and date of birth. As with other National Spine applications, access is controlled by a combination of smartcard privileges (Position Based Access Control or 'PBAC') and system control based on "legitimate relationships" with patients.

4.5.3.2 South Tees was the first acute trust in the North East to introduce the SCR into secondary care and worked collaboratively with Connecting for Health to produce a Business Change and Information Governance Model for Viewing Summary Care Records and a staff SCR e-learning module, for use by other Trust's nationally.

4.5.3.3 Currently staff in A&E, AAU Ward 1 (Female), AAU Ward 15 (Male), Ward 28 Elderly Care, Ward 3, Cardio, and Pharmacy are all accessing SCRs for a selection of their patients when required. The uptake and usage is consistent across these areas. The trust is hoping that there will be an increase in the upload of SCRs by GPs as the current upload stands at around 60%.

4.5.3.4 Organisations are required to have a Privacy Officer in place for monitoring and assurance purposes and this function is currently within the IG department. SCR access is monitored weekly by the Privacy Officer. Each access generates an alert which is matched against a report from the Trust's CaMIS system. Any anomalies are investigated and signed off by the Privacy Officer accordingly. Should any system access raise concerns then these will be escalated to the head of IG and Caldicott Guardian for review/action.

4.5.4 SystmOne Unit Transfer

4.5.4.1 A report was written in October 2011 to highlight the pending requirement to transfer selected SystmOne Units from the PCTs to South Tees as a result of the Transfer of Community Services. The paper highlighted the risks involved and provided options as to a way forward with the process. In October and November 2012, all community SystmOne units were transferred to South Tees using the Operation Data Service. Support for the units was provided by Tees PCT and North Yorkshire & York PCT as part of a service level agreement. The RA Manager worked closely with the PCT staff and relayed relevant information about the transfer of the SystmOne units back into South Tees.

4.5.4.2 As of April 1st 2013 RA / smartcard support from Tees PCT ceased. Therefore the Trust currently supports 32 active SystmOne units in the Redcar & Cleveland and Middlesbrough locations. There are 12 active SystmOne units in North Yorkshire & York which continue to be supported by the PCT under the current service level agreement.

4.6 IG Training Needs & Awareness

4.6.1 In line with recommendations in the Information Governance Assurance Programme and the NHS Operating Framework, information governance training became mandated for annual completion by staff. A key driver in support of this was the IG toolkit requirement for training, in which the trust was required to evidence that all staff (minimum 95%) had completed the mandatory information governance training module by 31st March 2013. Numerous briefings and bulletins were circulated by various methods to increase staff awareness on the required annual IG training

4.6.2 Mandatory training compliance is monitored by a team in Human Resources and compliance was confirmed at 87% at the end of March 2013, compared to 70% in March 2012**.**

4.6.3 The Information Governance team worked with the learning and development department to ensure that IG training once again formed part of the delivered corporate mandatory training (CMAT) across the trust. Individual/group sessions were regularly delivered across the community division as required.

4.6.4 The IG team introduced the use of "Train the Trainer" within divisions, providing a development opportunity for interested staff and with the added benefit of creating easy access to training within their divisions/directorates. This has been very successful in 2012/13 with table 10 highlighting the current take up.

Table 10

Division	Approved Trainers
Academic	x1
Acute Medicine	x6
Anaesthetics & Theatres	x1
Healthcare Governance	x1
IT & Health Records	x5
Neurosciences	x1
Planning	x1

Radiology	x1
Speciality Medicine	x1
Trauma	x1
Women and Children	x1

4.6.5 As the compliance rate was nearing the 95% minimum level, the trust submitted a level 2 compliance score on the provision that an action plan was in place allowing an extra 4 weeks to raise the percentage as much as possible. Compliance reports were sent to divisional managers, corporate directors and IG Leads on a weekly basis highlighting those staff whose training was still outstanding. At the end of April 2013 the trust achieved a final compliance score of 91.45% an increase of over 21% on 2011/12. The following table highlights the breakdown of methods of training and its % take-up throughout the Trust:

Table 11

Method of training	Number of Staff	%
Self Declaration	3463	39.98%
CFH Online Training Tool	796	9%
Other methods: (include CMAT, Delivered Sessions & Corporate Induction).	3662	42.00%
Non-Compliant staff	740	8.55%

4.6.6 Information governance also forms part of the trust's Risk Assessment Training Programme. This training gives awareness and guidance on how to conduct an Information Risk assessment as well as reporting and investigation of information incidents.

4.7 Transforming the Care We Deliver

4.7.1 Due to the significant changes in working practices and systems identified as part of this programme, specific information security guidance and review was required throughout the various stages of the contract. Some of the significant areas covered are highlighted below:

- Scoping Security Requirements
- Contract review
- Data Centre Reviews
- Help Desk Reviews
- Dialogue with bidders
- Reviews of ITPD1 and ITPD2

5. Information Governance Key Drivers and Work Plans for 2013/14

A high level Information Governance Action Plan has been developed (see Appendix B) which encompasses the trusts priorities and key milestones within the current IG Framework. A number of detailed actions plans are in place to support the high level plan.

5.1 Information Governance Department

5.1.1 To ensure that corporate services are working as effectively as possible, the Chief Executive and Director of IT & Health Records have discussed the recommendations regarding the strengthening of governance in light of the recent Sir Robert Francis report, as well as the synergy of the work of the IG team and the Quality & Assurance Directorate. With this in mind the IG department will transfer to Quality & Assurance

Directorate under Prof Wilson's leadership, where the team will continue to build upon the quality and service that is already provided to colleagues across the trust.

5.1.2 The IG department will review the feasibility of using the MIDAS system as a corporate IG tool. The review will align current processes of work and ensure a single robust system giving divisions/directorates a holistic view of their IG requirements and information such as FoIA requests, subject access requests, data flows, database registrations and Caldicott approvals. It is envisaged that this will act as a one-stop-shop allowing IG leads to collate, populate and review the divisional documentation required for IG toolkit evidence.

5.1.3 The IG department anticipates a significant role in a number of work streams for the Transforming the Care we Deliver Programme, but at the moment the areas and level of support is not defined.

5.2 Audit & Monitoring – IG Toolkit

5.2.1 The IG Toolkit v11 was released in June 2013 and is currently under review by the IG team to assess any changes in the requirements which may have an impact on establishing a new baseline for the Trust.
The Trust is required to report three times in year as follows:

- 31st July 2013 - Baseline assessment
- 31st October 2013 - Progress Update
- 31st March 2013 - Final submission

5.2.2 Appendix C highlights the IG toolkit v11 requirements and baseline scores for 2013/14. Due to the tight timescale for submission the baseline score may be based on the requirement scores submitted in March 2013. A full review of all standards is underway in preparation for the progress update in October 2013, allowing an improved understanding and trust position of IG compliance.

5.2.3 2013/14 will see the v11 IG Toolkit Work Programme integrated into the Trusts Health Assure system, and updated to evidence compliance against the standards.

5.2.4 The Information Governance Steering Group will monitor the High Level Action Plan and the IG Toolkit Work Programme, the minutes of which will be received into the Formal Management Group. The IG Toolkit submission scores will be presented to the Integrated Governance Committee to provide assurance that the trust is achieving the required level of compliance with legislation and national standards.

5.2.5 The Information Risk Management framework relies heavily upon the requirements of the IG Toolkit. Once v11 requirements have been reviewed, further guidance and/or actions to ensure compliance will be disseminated via the trust's IRM structure and divisional/directorate IG Leads.

5.2.6 Internal audit will review the trust's compliance against the IG Toolkit. A number of related audits will be included as part of the Trust's internal audit schedule.

5.3 Legislation, National Standards & Policy

5.3.1 The contract with commissioners requires the trust to reach a minimum level 2 on all IG toolkit standards.

5.3.2 Although Caldicott2 recommendations remain high level at present the trust will review and consider implementation where possible as good practice. This will be taken forward as part of the IG High Level Work Programme 2013/14 and may require a more detailed action plan with work streams and key dependencies where necessary.

5.3.3 The IG department will keep abreast of events in Europe with regards to pending EU Data Protection Reform. Once modifications are confirmed, and it appears likely that such changes will be reflected in UK law, a report for organisational information/consideration will be provided as appropriate.

5.3.4 The information governance/Toolkit v11 requirements will feed into the following governance arrangements where required:

- Statement of Internal Control.
- Trust Annual Plan.
- Trust Annual Report
- Care Quality Commission (CQC).
- NHS Quality Accounts

5.3.5 An IG Policy Plan is in place to continue the review/development of policies.

5.3.6 A review of the trust's overarching IG Policy will take place to ensure an appropriate and robust information governance framework across the Trust.

5.4 Confidentiality & Data Protection Assurance

5.4.1 The Health & Social Care Information Centre (HSCIC) has reviewed and re-issued guidance in June 2013 regarding *Reporting, managing, and investigating information governance serious incident.*[6] This guidance requires a whole new way of coding serious incidents, now known as a *Serious Incident Requiring Investigation* (SIRI), with regards to data breach and data loss. This is currently causing much discussion within the NHS and Social Care, particularly around the grading of incidents (now level 0-2 instead of 0-5) as it is envisaged that more incidents will be reported to the ICO due to a perceived lower risk threshold.

5.4.2 From June 2013 all organisations processing health and adult social care personal data are required to use the IG Toolkit Incident Reporting Tool to report level 2 IG SIRIs to the Department of Health (DH), ICO and other regulators.

5.4.3 A Memorandum of Understanding is in development between the DH, HSCIC and the ICO to share intelligence on IG SIRIs for the purpose of supporting, guiding, investigating breaches, performance monitoring and improving standards of health and adult social care services.

5.4.4 Local clinical and corporate incident management and reporting tools (including Strategic Executive Information System - STEIS) can continue to be used for local purposes but notifications of IG SIRIS for the attention of DH and the ICO must be communicated using the IG Incident Reporting Tool with immediate effect.

5.4.5 As well as the above there is considerable change in regards to the way NHS organisations should code IG incidents. A full review of the recent guidance is underway and an implementation plan will be developed to assure the required changes are reflected as necessary.

5.4.6 The development of this guidance and the new IG Incident Reporting Tool involved representatives from the NHS, DH IG & Standards Policy and the ICO Enforcement Department. The ICO's Office supported this move with the following statement:

… *"The health sector routinely handles extremely sensitive personal data, and it is essential that such information is looked after appropriately. On the occasion where that has not been achieved, it is important that the relevant authorities are made aware at the earliest opportunity. The National Health Service (NHS) has an established culture of informing the ICO of all data breaches, and we welcome the new incident*

[6] https://nww.igt.hscic.gov.uk/resources/IGIncidentsChecklistGuidance.pdf

reporting tool which will mandate that reporting process and make it simpler and more efficient.

The ICO has worked closely with the Health and Social Care Information Centre to support the development of the reporting tool and we anticipate that it will become a useful resource for information governance professionals within the NHS"…

5.4.7 The IG team will continue to raise awareness of incidents via the trust STARS system (Risk Alerts/Updates) and all-user briefings where necessary, to help mitigate the risk of similar incidents being repeated. The IG department will also review the ICO Monetary Penalty Notices to ensure that any lessons learned from these incidents can be shared and acted upon within the trust where necessary.

5.4.8 The information governance department are currently progressing the standardisation of data protection and subject access request processes across the organisation to ensure consistency in compliance with the Act. An implementation plan is in place to ensure further phases are completed as required.

5.4.9 The IG team will work with IG leads to instigate data protection audits within their areas. As the ICO may be granted an extension to powers to carry out non-consensual audits on any NHS organisation, these will help assure divisions and directorates on their current IG compliance and help highlight any areas that need further consideration with regards data protection/information risk.

5.4.10 The need to evidence service user satisfaction with regards to confidentiality will be undertaken via patient satisfaction surveys led by Quality & Assurance.

5.4.11 The IG department will keep a register of current information sharing agreements, providing support and guidance to staff with regards to the creation of agreements where necessary.

5.5 Corporate Information Assurance

5.5.1 The FoIA statutory 20 day timeframe for responding to requests will continue to be monitored by the IG Steering Group and reported into the Formal Management Group through quarterly compliance reports by the SIRO.

5.5.2 Records Management

5.5.2.1 The Records Management Strategy, supported by policy and associated standard operating procedures, will be escalated across the trust with divisional/directorate IG leads advised of necessary work programmes.

5.5.2.2 IG will advise divisional/directorate IG leads on records audits to support identification and registration of divisional information assets.

5.5.3 The Protection of Freedoms Act 2012

5.5.3.1 The trust is awaiting national guidance on the publication of datasets and enforcement of the Protection of Freedoms Act 2012. It is envisaged that this requirement is likely to place a burden on some corporate directorates who routinely produce data sets in that these will have to be published on the trust's website and updated whenever a revised dataset has been compiled.

5.6 Information Security & Information Risk Management Assurance

These two requirements run in tandem and will be combined within the Project Plan for 2013/14.

5.6.1 The IG department will revisit Information Risk Management requirements across the organisation in light of v11 of the IG Toolkit.

5.6.2 Information risks will be reviewed and monitored by the Information Governance Steering Group. The SIRO will feed any Information risks/concerns into the Risk & Assurance sub-committee for discussion and escalation from local risk to corporate risk where appropriate.

5.6.3 The IG department will devise a schedule for trust systems to ensure that the appropriate system specific security documentation is complete and robust including IT business continuity and disaster recovery plans.

5.6.4 A series of audits are planned to be performed across the trust to ensure that PC's and current Trust approved mobile equipment conforms to trust policy.

5.6.5 The trust has identified a solution to implement mobile device management to ensure that the security of network connections, patient identifiable, business sensitive and confidential information can be appropriately contained. IG will ensure a secure framework is developed and established.

5.6.6 IG will establish a framework for the use of social media. A policy will be devised in conjunction with human resources and public relations. This will help to ensure that staff are aware of, and comply with, the appropriate guidance available when using social media in both a personal and a professional capacity.

5.7 Connecting for Health / Health and Social Care Information Centre Update

5.7.1 Registration Authority & Integrated Identity Management

5.7.1.1 A new RA Agent post is in the process of being recruited into the Application Support team in ICT to facilitate the management of smartcards and general RA processes across the trust. This role will be key in the further development of the interface between the Electronic Staff Record (ESR) and the User Identity Manager (UIM) system used to create smartcards. It will also ensure consistent use of Position Based Access Control (PBAC) and work closely with the community staff to ensure SystmOne access and workgroup allocation is correct and in line with governance.

5.7.1.2 As part of the Choose and Book referral project, RA super-users have been set up across divisions. These super-users will be able to unlock and renew smartcards on an ad hoc basis.

5.7.3 Summary Care Record Implementation

5.7.3.1 Summary Care Record (SCR) access is now used on several wards and departments across the trust. A planned roll-out will continue in conjunction with IT.

5.7.3.2 It is anticipated that the Privacy Officer role will increase to embrace Caldicott2 recommendations building "Privacy by design" into the new electronic patient record systems as part of the Transforming the Care we Deliver Programme.

5.8 IG Training & Awareness

5.8.1 Information Governance training is mandated annually by the Department of Health. In order to help the trust reach level 3 on the IG Toolkit, a minimum of 95% of staff trained in IG is required. IG training can be accessed by either online training or by attendance at a delivered session facilitated by a member of the IG team or an appropriate divisional/directorate IG trainer. A power point presentation, test and declaration is also available.

5.8.2 The trust IG Leads Forum acts as a medium for training and awareness sessions and allows constructive feedback from operational staff. The IG department will look to build on the development of divisional/directorate IG trainers to allow all staff easier access to area specific IG training.

5.8.3 Information governance is everyone's responsibility and all staff are required to undertake IG training appropriate to their role. In order to achieve robust information management and a reduction in information incidents there needs to be engagement and understanding across the trust. Having access to topic specific training will allow staff to undertake "advanced" training specific to their role within the organisation, helping to build on staff awareness and understanding of information governance. Guidance on role specific IG training now forms part of the mandatory training and development prospectus published by Human Resources.

5.8.4 The IG Department will continue to raise awareness of local and national IG issues/concerns by working with all staff and divisional/directorate IG leads. This will be achieved by issuing monthly compliance reports highlighting non-compliant staff, targeting individual wards and departments, offering individual group training and ad-hoc drop in sessions, advising staff in advance of when local CMAT sessions are to be held, issuing updates in the staff bulletin and also the IGEye quarterly bulletin. The IGEye provides a "one stop update" on IG issues and hot topics for local team briefings.

5.8.5 An annual training plan will be developed in conjunction with IG leads and will be monitored by the IG department and the IG Steering Group for assurance.

6. <u>Risks to Achievement</u>

6.1 A key risk will be continuing to maintain a minimum of Level 2 compliance on all IG Toolkit v11 standards across the organisation. Having achieved this level, the trust now needs to maintain it and build upon past success achieving level 3 in key areas.

6.2 Corporate IG processes and requirements need to be reviewed across the organisation to ensure that the Trust remains compliant with its statutory and national obligations. Key identified risk/considerations include:

1. Consistent approach to the management of information requests and archived information.

2. An integrated system for recording
   - Subject Access Request,
   - Freedom of Information Requests
   - Environmental Information Requests (EIR)
   - Information Assets
   - Dataflows/Audits

6.3 For community services all of the above are recorded electronically within a single system (MIDAS); however this system is not available across the rest of the trust. This presents a risk to the organisation and the options for introducing a central IG repository needs further consideration.

6.4 Due to the impending ICO review of acute trusts publication schemes and the enactment of the Protection of Freedoms Act 2012, the organisation needs to ensure that it has a publication scheme in place and that all information required via the internet is up-to-date. Non-conforming organisations will be contacted by the ICO directly. The Trust therefore needs to ensure that its information for the public is published routinely and consistently.

6.5 Although the IG department has recruited some divisional IG trainers, the trust still relies on staff taking the responsibility for completing the training themselves. Training will be monitored and reported to divisional managers and corporate directors to ensure that IG training is undertaken in order to reach the continuous 95% level 2 requirement.

6.6 Information risk management, including asset ownership, like any culture change has taken time to embed into the organisation. Accountable staff need to ensure that information risk and asset management/ownership responsibilities are administered effectively and not seen as an IT/IG responsibility. An appropriate system and process needs to be in place to ensure the robust management of trust information assets.

6.7 The IG agenda is large and complex with ever increasing demands on the service. Transforming the Care we Deliver Programme and other unexpected demands will need to be taken into consideration, and may affect the delivery of the IG development plan for 2013/14.

6.8 In light of the pending ICO powers to audit NHS organisations it is strongly recommended that data protection audits are undertaken within divisions to understand and mitigate any highlighted areas of non-conformance with the Act.

6.9 The volume of complex subject access requests could risk scrutiny by the ICO should a complaint be made. These pose a significant strain on the department with regards to timescales and resource due to a number of factors such as records management issues (particularly emails) and redaction of 3rd party information where appropriate.

7. Summary

7.1 This report sets out what has been achieved within the IG Programme for 2012/13. This year has again seen a rapid increase in demand on the resources dedicated to the IG programme and the team has worked hard to ensure that the trust has kept up with the pace of the demands of the national information governance agenda, in addition to the day to day operational aspects of IG.

7.2 For the first time in a number of years the trust achieved the minimum level 2 on all requirements of the IG Toolkit as well as receiving the first full assurance audit report from Audit North.

7.3 More importantly this report sets out a work programme to further enhance a robust IG framework within the trust for 2013/14. The year's priorities focus further on information risk management and incident reporting and ensuring that processes are in place to support patient rights, confidentiality and data security and accessibility.

7.5 This year the trust may see a significant change to IG collectively, through NHS review/reports such as Caldicott2 and Francis, as well as pending legislative changes via the EU data protection reforms. As the visibility of IG is raised, so are the demands on the service. Activity is constantly increasing and the organisation needs to ensure that information governance is managed in a robust way within work areas and not seen as something that is the sole responsibility of the IG department.

7.4 Information Governance forms part of the Integrated Governance Framework and the one thing that is certain, is that this already large and complex agenda, still gains momentum. Public interest will continue to rise through the media reporting of adverse events, as seen in the ICO monetary penalty notices for data loss/breach. Going forward, the IG team will continue to monitor how the ICO applies its Regulatory Powers (particularly to the NHS) with regards to penalty notices for data loss incidents. Where appropriate, the learning will be used to reduce any potential risk to the trust. Should the ICO gain powers for non-consensual audits of NHS organisations, it will be interesting to see, how this power is applied and its effect, particularly within health and social care settings.

7.5 The Board of Directors is asked to:

- note IG progress in 2012/13
- approve the High Level Project Plan (app. B)
- note the IG Toolkit baseline score for July's required submission. (app. C)

(Appendix A)

GLOSSARY

Abbreviation	Term
CfH	Connecting for Health
DPA	Data Protection Act 1998
e-GIF	e-Government Interoperability Framework – Levels 0-3. e-GIF level 3 compliant – identity proven 'beyond reasonable doubt', evidenced by three forms of identification.
ESR	Electronic Staff Record
FoIA	Freedom of Information Act 2000
IAA	Information Asset administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
IIM	Integrated Identity Management – a single rigorous identity check for employment purposes
ISA	Information Sharing Agreement
IT	Information Technology
PBAC	Position Based Access Control –system access level, determined by the users defined role in ESR
RA	Registration Authority – the Trust's arrangement for the issuing and management of smartcards
SCR	Summary Care Record – national clinical system
SIRO	Senior Information Risk Owner
Smartcard	A plastic card used to control access to the NHS Care Records Service
SOC	Statement of Compliance
SIRI	IG Serious Incident Requiring Investigation (previously a SUI)
SOP	Trust Standard Operating Procedure
UIM	User Identity Manager – system used to create Smartcards

(Appendix B)

Information Governance High Level Project Plan – 2013/14

Key Driver	Key Actions	Responsibility	Timescale
Audit & Monitoring	Update Work Programme for IG Toolkit v11	Head of IG Deputy IG Manager	Jul 2013 Oct 2013 Mar 2014
	Develop and distribute Divisional/Directorate IG Toolkit action plans to aid collation and monitoring of evidence and attainment levels	Deputy IG Manager	Aug 2013
	To aim for level 3 scoring on all Information governance Toolkit Standards (Minimum level 2 required)	Head of IG Deputy IG Manager	Mar 2014
	Verification of IG Toolkit scores and evidence	Head of IG / Financial Services Manager	Mar 2014
	Audit North to audit IG Toolkit scores and evidence	Head of IG / Audit North	Mar 2014
	Undertake required continuous testing audits	Head of IG/ Audit North	Jan 2014
	Review overarching IG policy to ensure appropriate and robust IG framework across the Trust IG groups in light of IG agenda and Trust Information Strategy	Head of IG	Oct 2013
	Transforming the Care we Deliver – IG Involvement • contract requirements • IG schedules & SLA requirements • transition & integration • projects & implementation • audit & monitoring	Head of IG Deputy IG Manager	On-going
	Review the feasibility of using the MIDAS system as a corporate IG tool	Head of IG	Sep 2013
Legislation, National standards & Policy	Review of Information Governance Incident Reporting framework in light of new HSCIC requirements. Including review of Datix reporting codes	Head of IG	Nov 2013
	Review, consider and implement recommendations from Caldicott2 as good practice where possible.	Head of IG	Mar 2014
	Review/develop Information Governance Policies& Standard Operating Procedures	Head of IG	On-going
	Align other National Standards into IG Toolkit Work Programme where appropriate	Head of IG	Mar 2014
	Review of the Protection of Freedoms Act 2012 and advise the Trust on compliance requirements	Head of IG	National guidance pending
	Review ICO Monetary Penalty Notices to ensure lessons learned can be shared and acted upon within the Trust where necessary.	Head of IG	On-going

Information Governance High Level Project Plan – 2013/14

Key Driver	Key Actions	Responsibility	Timescale
Confidentiality & Data protection Assurance	Review of the Data Protection Act, subject Access Request Processes.	Head of IG	Oct 2014
	Trust Data Protection Audit • 2013/14 DPA survey • Supporting Divisional/Directorate DPA audits • Service user DPA satisfaction audit	Head of IG	Feb 2014
	Review and update South Tees DP Notification to the ICO where appropriate	Head of IG	Sep 2013
	Trust register of Information Sharing Agreements, providing support and guidance to staff with regards the creation of agreements were required.		Sep 2013
Corporate Information Management	To work with Divisional IG representatives to audit and register divisional information assets	Head of IG	Mar 2014
	To advise the organisation on Publication Scheme requirements as stated under the Freedom of Information Act 2000.	Head of IG	Mar 2014
	Monitor divisional/directorate compliance against statutory 20 day timeframe as stated under The Freedom of Information Act 2000	Head of IG	On-going
Information Security & Information Risk Management Assurance	Work with and support System IAA's to ensure the required system documentation is in place.	Deputy IG Manager	Mar 2014
	To undertake IT Business Continuity as part of the trust wide business continuity Programme of work	Deputy IG Manager	Mar 2014
	To advise and support the Trust on mobile device management	Deputy IG Manager	Nov 2013
	Continued advice and support on the Trust's management and use of its social media.	Deputy IG Manager	On-going
	Revisit and support divisions and directorates on Information Risk management requirements across the Trust	Deputy IG Manager	Nov 2013
Connecting for Health & National Programme for IT Registration Authority	Roll-out of Summary Care Record (SCR)	Head of IG	On-going
	Access Control/RA Agent and Super-user functionality to be established within the organisation to support national systems i.e. SystmOne.	Head of IG/ IT Manager	Nov 2013
	Privacy Officer role to embrace Caldicott2 recommendations building "Privacy by design" into the new electronic patient record systems as part of the Transforming the Care we Deliver Programme.	Head of IG	Currently TcWD dependant
IG Training & Awareness	Trustwide awareness on IG including local and national issues	Deputy IG Manager	Ongoing

Information Governance High Level Project Plan – 2013/14			
Key Driver	**Key Actions**	**Responsibility**	**Timescale**
	Review IG mandatory training requirements to ensure - All staff (min 95%) complete annual training - IG training plan in conjunction with IG leads - IG forms part of the corporate TNA to ensure compliance with IG toolkit requirements. - build on the development of divisional/directorate IG trainers to allow all staff easier access to area specific IG training.	Deputy IG Manager	Mar 2014
IG Department	Review the department in line with the continuing developments of the IG agenda.	Head of IG	On-going

(Appendix C)

2013/14 Baseline Score for South Tees NHS Foundation Trust

Req No	Description	Status	Attainment Level
Information Governance Management			
11-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Reviewed	Level 3 ✓
11-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Reviewed And Updated	Level 3 ✓
11-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	Reviewed	Level 2 ✓
11-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	Reviewed	Level 3 ✓
11-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Reviewed And Updated	Level 3 ✓
Confidentiality and Data Protection Assurance			
11-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	Reviewed	Level 3 ✓
11-201	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users	Reviewed And Updated	Level 3 ✓
11-202	Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected	Reviewed	Level 2 ✓
11-203	Individuals are informed about the proposed uses of their personal information	Reviewed	Level 2 ✓
11-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Reviewed	Level 2 ✓
11-206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	Reviewed And Updated	Level 3 ✓
11-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	Reviewed	Level 2 ✓
11-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Reviewed	Level 2 ✓
11-210	All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements	Reviewed	Level 2 ✓
Information Security Assurance			
11-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	Reviewed	Level 3 ✓
11-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Reviewed	Level 2 ✓
11-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Reviewed	Level 2 ✓
11-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	Reviewed	Level 3 ✓
11-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	Reviewed	Level 3 ✓
11-305	Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems	Reviewed	Level 2 ✓
11-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	Reviewed	Level 2 ✓
11-308	All transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational	Reviewed	Level 2 ✓

	measures adequately secure these transfers		
11-309	Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures are in place	Reviewed	Level 2 ✓
11-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Reviewed	Level 2 ✓
11-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	Reviewed	Level 2 ✓
11-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Reviewed	Level 2 ✓
11-314	Policy and procedures ensure that mobile computing and teleworking are secure	Reviewed	Level 2 ✓
11-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Reviewed	Level 2 ✓
11-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Reviewed	Level 2 ✓
Clinical Information Assurance			
11-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Reviewed	Level 2 ✓
11-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Reviewed And Updated	Level 2 ✓
11-402	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care	Reviewed	Level 2 ✓
11-404	A multi-professional audit of clinical records across all specialties has been undertaken	Reviewed	Level 2 ✓
11-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	Reviewed	Level 2 ✓
Secondary Use Assurance			
11-501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop	Reviewed	Level 2 ✓
11-502	External data quality reports are used for monitoring and improving data quality	Reviewed	Level 2 ✓
11-504	Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained	Reviewed	Level 2 ✓
11-505	An audit of clinical coding, based on national standards, has been undertaken by a NHS Classifications Service approved clinical coding auditor within the last 12 months	Reviewed	Level 2 ✓
11-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	Reviewed	Level 2 ✓
11-507	The Completeness and Validity check for data has been completed and passed	Reviewed	Level 2 ✓
11-508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity	Reviewed	Level 2 ✓
11-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national standards	Reviewed	Level 2 ✓
Corporate Information Assurance			
11-601	Documented and implemented procedures are in place for the effective management of corporate records	Reviewed	Level 2 ✓
11-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Reviewed And Updated	Level 2 ✓
11-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	Reviewed	Level 2 ✓