Northumbria Healthcare NHS
NHS Foundation Trust

Report to the Information Management & Technology Group **Enc 11**

Title of Report	Senior Information Risk Owner (SIRO) Report
Author	Tracey Best, Information Governance & Projects Manager
Executive Lead	Mark Thomas, Director of Informatics
Date of meeting	8th March 2017
Executive Summary	This report is to provide assurance to the Trust in relation to the effectiveness of controls for Information Governance (IG), data protection and confidentiality. This assurance is provided by the Senior Information Risk Owner (SIRO) who has executive responsibility for information risk and information assets. The SIRO is support in this work by the Information Governance Group which meets bi-monthly. This report covers the following areas: • Implementation of the IG Strategy & Framework • The work of the IG Group • Progress with the IG Toolkit action plan and collation of evidence to support v14 IG toolkit submission by 31 March 2017 • IG Training • Freedom of Information Requests • IG incidents and breaches
Assurance Framework reference	Assurance against Information Governance requirements placed on the Trust, particularly by the Information Governance Toolkit and Care Quality Commission.
Alignment to Trusts Annual/Strategic Plans or business unit annual plans	N/A
Risk rating (very high, high, medium, low risk)/ any recommended changes	N/A
Compliance/ regulatory requirements (if	Compliance with legislation, including but not limited to the Data Protection Act 1998 and the Freedom of

applicable)	Information Act 2000.
Actions required by the Committee	The Group is asked to note the activity outlined in the report.

Senior Information Risk Owner (SIRO) Annual Report 2016-17

1. Introduction & Purpose

1.1 This report is to inform the Board of progress against the Information Governance (IG) work programme in 2016-17 and to outline the key priorities and associated work programmes for 2017-18.

1.2 The Trust currently has an Information Governance Sub Committee to provide advice and assurance to the Trust on all matters concerning information governance.

1.3 Throughout 2016-17 there has been continuing progress in improving the effectiveness and raising awareness of the organisational Information Governance mechanisms.

1.4 This report summarises the main themes of the programme and work undertaken in Information Governance during this period.

1.5 The report comments on:

- Compliance with the Information Governance toolkit and improvements in relation to managing risks to information
- Organisational compliance with legislative and regulatory requirements relating to handling of information, including compliance with the Data Protection Act (1998) and Freedom of Information Act (2000)
- Any Serious Untoward Incidents within the preceding twelve months, relating to any losses of personal data or breaches of confidentiality
- Implementation of Caldicott 2, 7th principle – duty to share, Health and Social Care (Safety and Quality) Act 2015 and the revised NHS Constitution (July 2015)
- The direction of information governance work during 2016-17 and how it aligns with the strategic business goals of the Trust and outlines the work plan for the coming year.

2. Information Governance Strategy & Framework

2.1 Information is a vital assess and needs to be managed securely by NHS organisations. Appropriate policies, guidance, accountability and structures must be in place to manage the Trusts information legally, securely and effectively in order to minimise risk to patients, public and staff and to protect its finances and assets.

2.2. The IG Strategy & Framework describes the Trust's approach to meeting its statutory duties in relation to information governance, data protect and confidentiality and has been refreshed to take into account new legislation – Caldicott 2, 7th principle – duty to share, the Health and Social Care (Safety and Quality) Act 2015 and the revised NHS Constitution (July 2015) i.e.

- Patients have the right to privacy and confidentiality, to expect the NHS to keep patient confidential information safe and secure, and to be informed about how their information is used;
- For the purpose of **direct care** relevant personal confidential data should be shared among the registered and regulated health and social care professionals (organisations) who have a **legitimate relationship** with the individual.

2.3 The suite of IG policies and procedures have also been reviewed to take into consideration the new legislation and good practice guidance.

3. Information Governance Progress 2015-16 (Version 13 IG Toolkit)

3.1 The Trust undertook its self-assessment against version 13 of the IG Toolkit in March 2016 and reported level 2 or above against all requirements and submitted at 94% overall ‘satisfactory’. The scores for each initiative are detailed below:

Information Governance Management	100% (Green)
Confidentiality and Data Protection Assurance	100% (Green)
Information Security Assurance	97% (Green)
Clinical Information Assurance	86% (Green)
Secondary Use Assurance	87% (Green)
Corporate Information Assurance	100% (Green)

4. Information Governance Assessment 2016-17 (Version 14 IG Toolkit)

4.1 The Information Governance Sub Committee will be approving version 14 IG Toolkit submission early March for 2016-17. A full assessment of the breakdown of scores will not be available until the scores have been submitted electronically.

4.2 We are currently on track to achieve level 2 compliance against requirements with the following challenge:

- 112 – Training. This requirement sets out that 95% of staff must complete IG training. This continues to be a challenge for the Trust; however this is monitored by Workforce Committee throughout the year.

4.3 An evaluation was carried out by internal audit in January 2017 of the proposed annual IGT submission and the Trust is awaiting the management response. .

5. Information Governance Sub Committee

5.1 The Information Governance Sub Committee has continued to raise its profile as the organisational focus for all matters relating to information governance, records management, data governance, security and confidentiality. The Sub Committee has continued to see a drop in attendance and representation in recent times which is currently being reviewed but this has not had any major impact on continuous improvements to the organisational IG mechanisms and processes. The Information Governance Sub Committee oversees the successful implementation of the IG Annual Work Programmes, and has been an effective forum for debate and decision making.

5.2 The 2016-17 Annual Work Programme is well underway and progress against this plan is being monitored by the Information Governance Sub Committee and update reports provided to the IM&T Committee.

5.3 Data Governance tables have been developed for each Business Unit and are reported regularly at the Information Governance Sub Committee.

6. Incident Management

6.1 There are formal arrangements to identify and mitigate risk in accordance with NHS information governance requirements and there are effective mechanisms in place to report and manage serious untoward incidents.

6.2 From June 2013 organisations have reported IG SIRIs to the Department of Health via the Information Governance Toolkit incident reporting tool and this has been further developed to include a section specific to Cyber Security incidents.

6.3 The severity of incidents reported via this tool are determined by the scale (numbers of data subjects affected), sensitivity factors selected and whether a similar incident has occurred in the last 12 months. If the outcome in terms of the severity of the incident is IG SIRI level 2 (reportable) an email notification is sent to the HSCIC External IG Delivery Team, Department of Health, Information Commissioners Office and escalated to other regulators, as appropriate.

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

6.5 During 2016-17 there were 4 serious incidents requiring investigation reported for the Trust. All 4 incidents involved in-appropriate access of confidential information.

6.6 Information governance incidents must be reported by public bodies in their annual reports; those with a higher severity rating (in effect those where data on more than twenty individuals are involved) must be report individually in a specified table, whilst those involving the data of twenty or fewer must be listed in an aggregated table.

6.7 The HSCIC is delivering a number of projects around cyber security education, awareness and training and enhancing their existing cyber security capabilities as a trusted centre of cyber security expertise.

6.8 The HSCIC has developed a Care Computer Emergency Response Team (CareCERT) and CareCERT will offer advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats.

6.9 The IG Sub Committee also routinely reviews the log of incidents raised for review by the Caldicott Guardian. Acting as the ‘conscience’ of the organisation, the Caldicott Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

7. Training

7.1 A programme of training sessions (supplemented by specific training for particular services or staff groups) is in place and an Information Governance awareness session is also given at induction. The IG team are currently working with the HR Training team to review the content and delivery of training.

7.2 Action plans are in place and are being monitored monthly by Workforce Committee to ensure compliance.

8. Information Risks

8.1 There are currently 33 Information Governance risks on the risk register and these have been summarised as follows:

- Training

- Compliance against 95% target for IG Training – moderate
- Merging fields in Word within SystmOne – Low Risk - The word document is changed when internal and external services updates information therefore not retaining the original document e.g. letter sent to patients. Staff training issue - low

- FOI
  - Non Compliance of FOI legislation not meeting statuary obligations - moderate

- Health records Cobalt
  - The main library at Cobalt has reached and exceeded full capacity risk of injury to staff – high
  - Old bar Code label on third of records unable to use scanning software – moderate

System / software risks

- Patient Alerts not shared or recorded on all Key systems - moderate
- JELS referral software creates a copy for Occupational therapists in my documents on c\:drive low
- Macros switched on in Word – ability to run malicious software without prompt - moderate
- Some PCs and servers not having AV in place – low

Infrastructure –

- Routing of email to personal and corporate devices is via an unsecure route due to inability to test changes to MDM server, as test server in place but resource issue staff to make changes – high
- No monitoring of databases for SQL injection attacks moderate
- Penetration test failings some issues awaiting infrastructure upgrades - high
- NHS Digital Security Alerts – Resource issues - low
- Ironmail – PID emails sent without being intercepted – software replacement in progress - moderate

PAS

- Record Access Audit Trail works with NHS number as identifier – with Scottish Patients this does not provide audit ability – moderate risk
- Two identifiers in PAS – Trust No and NHS No – noncompliance with national requirements for NHS No to be key identifier – moderate risk

System level Security – key systems

- No formal process within Maternity (E3) to change access rights - moderate
- ICE unable to be tested to meet Trust Password Policy – moderate
- ICE unable to follow 3rd Party Trust Procedure – moderate
- ICE Numerous generic accounts - moderate
- Generic accounts within ICE (Under review) – moderate
- G2 temporary contract until April 17 - low
- Somerset, system is not able to provide failed logon reports – moderate
- There are currently issues with the creation of duplicate and triplicate registrations in Euroking. Moderate
- POAS and CAHMS NHS number not verified and validated moderate
- IAPTUS not able to provide failed logon reports – moderate
- IAPTSU no evidence of being able to regress - moderate
- E3 not able to provide failed logon reports - moderate
- Patient Browser not able to provide reports on access - moderate
- Medispeech and sexual health letters to GPs – low
- Merger of Blithe Lillie to S1 – moderate

9.1 During 2016-17 (to 31st Dec 2016) the Trust received 519 requests under the provisions of the Freedom of Information Act 2000 which is an increase of 106 in comparison to the first three quarters of 2015-16.

9.2 The table below shows the quarterly breakdown of requests and response times.

	On time	% on time	Over 20 day limit	% over time	Totals 2016-17	Totals 2015-16
Quarter 1	64	35.36%	141	77.90%	181	128
Quarter 2	61	34.36%	116	65.54%	177	144
Quarter 3	57	34.40%	104	64.60%	161	141
Quarter 4	N/A	N/A	N/A	N/A	N/A	152
Overall	**182**	**35.06%**	**361**	**69.55%**	**519**	**565**

*Quarter 4 not complete

9.3 Performance against response times remained unsatisfactory during the year. Compared to previous years the nature of requests have been more complex and several required in-depth investigation to find detailed information and subsequently greater review of that information and any exemptions that apply prior to disclosure. Furthermore it is still difficult to obtain information in the statutory time period back from leads and resources/capacity has played a detrimental impact on the ability to monitor the FOI's until recently.

9.4 There were 5 main themes of information requested:

- IT and Telecoms
- Contracts – Various areas
- Staff costs – Agency/Locum
- Pharmacy/Medical Equipment
- Staff Figures i.e. F1's/F2's

9.5 During 2016-17 (to 31st December 2016) the number of subject access requests for record for 2015-16 was 95 compared to 63 for the same 3 quarters of 2015-16 which represents an increase of 32 requests.

The table below sets out the quarterly breakdown of requests and response times:

	On time	% on time	Over 40 day limit	% over time	Totals 2016-17	Totals 2015-16
Quarter 1	27	81.81%	2	06.06%	33	23
Quarter 2	35	87.50%	4	10.00%	40	12
Quarter 3	17	60.71%	0	0%	22	28
Quarter 4	N/A	N/A	N/A	N/A	N/A	35
Overall	**79**	**83.15%**	**6**	**06.31%**	**95**	**98**

*Quarter 4 not complete

10. Strategic Direction

10.1 The Trust has a dynamic action plan to refresh and improve its compliance with the IG Toolkit standards. This will be formally reviewed once the toolkit is published for the year ahead (2017-18).

10.2 Evidence for many of the toolkit requirements is readily refreshed as part of established daily business or monitoring activities. However, some objectives are harder to achieve and for this reason they are being targeted early on.

10.3 The Information Governance function will continue to work across all areas of the organisation to:

- Actively support the delivery of strategic priorities.
- Continue to work towards, achieving “Green” status for the Trust in national IG ratings.
- Work collaboratively with partner organisations to achieve continuous improvements in meeting national, statutory, and good practice requirements.
- Implement effective mechanisms for achieving compliance with changing statutory requirements e.g. FOI, data security.
- Undertake continuous assessment and report on risks associated with information systems, data, and processes through the established risk management mechanisms.
- Continue to work closely with IT staff to implement and provide continuing support to new clinical and corporate records systems.
- Continue to raise levels of awareness amongst staff of their information governance responsibilities by the delivery of effective training and communications and play a key role in supporting staff training and development.

10.2 Following the publication of version 14 IG Toolkit a high level Information Governance Action Plan will be developed which will encompass the Trusts priorities and key milestones within the current IG framework.

10.4 The Government has mandated NHS England to improve health outcomes and the quality of patient care through digital technology and innovation. The NHS will be paperless by 2020 (“Personalised Health and Care 2020”), and the Trust is working with partners across the region in delivering the “Digital Roadmap”, as part of new models of care programme.

10.5 The government has now confirmed that the UK will be implementing the General Data Protection Regulations (GDPR). According to the Secretary of State Karen Bradley MP “We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public”. On the 25 May 2018, the GDPR, or something very similar to it, will apply. The UK might retain the GDPR in full, or it might adopt GDPR-lite or even DPA-plus. The Trust is required to ensure that all amendments to processes are carried out to limit the risk of possible breaches and action plan will be developed to ensure appropriate actions are taken to implement the GDPR.

11. Summary

11.1 This report highlights the achievements made by the Trust within the IG Programme for 2016-17. The IG 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.

11.2 The Trust’s standard of Information Governance remains at a high level and this is represented in the annual returns. This level of compliance is attributed to the effective management of the IGT requirements.

11.2 Due to the increasing national and international news coverage regarding recent information security breaches of personal information, there is a heightened awareness of the requirement for robust information governance and security processes. The requirements to ensure that the security of personal identifiable, confidential or sensitive information accessibility, through NHS IT systems and whilst in transit remains of overriding importance.

11.3 The IG framework is already a large and complex agenda which we expect will continue to gain momentum. Public interest will continue to rise through the media reporting of adverse events and the proactive increase of awareness planned by the Information Commissioners Office, Data Guardian Report and the new GDPR regulations. Going forward, the IG team will review national guidance issued in support of changes to legislation and monitor how the ICO applies its Regulatory Powers with regards to penalty notices for data loss incidents and where required, continue to apply the learning to ensure risk mitigation within the Trust.

The Board is to note the Senior Information Risk Owner (SIRO) Annual Report and Information Governance strategic direction.