Yorkshire Ambulance Service NHS
NHS Trust

An Aspirant Foundation Trust

MEETING TITLE Trust Board		**MEETING DATE** 30/09/2014	
TITLE of PAPER	Annual Review of the Adequacy of the Information Governance Management Framework, Role of the SIRO and Supporting Information Risk Management Infrastructure.	**PAPER REF**	4.3
STRATEGIC OBJECTIVE	Develop culture, systems and processes to support continuous improvement and innovation To provide services which exceed patient and commissioner expectations		
PURPOSE OF THE PAPER	The purpose of this paper is to review the adequacy of the Information Governance Management Framework and ensure it remains fit for purpose. In addition the purpose is to ensure the role and responsibilities of the Senior Information Risk Owner and supporting information risk management infrastructure i.e. Caldicott Guardian, Registration Authority Lead and Information Asset Owners, remain current, effective and correctly assigned.		
For Approval	☒	**For Assurance**	☒
For Decision	☒	**Discussion/Information**	☐
AUTHOR / LEAD	Information Governance Manager	**ACCOUNTABLE DIRECTOR**	Executive Director of Standards & Compliance
DISCUSSED AT / INFORMED BY – This paper forms part of an annual requirement of the Information Governance Toolkit to review the adequacy of the information governance management framework, role of the SIRO and supporting information risk management infrastructure.			
PREVIOUSLY AGREED AT:	**Committee/Group:** Not Applicable	**Date:**	
RECOMMENDATION	The Trust Board notes the current arrangements and agrees that the Information Governance Management Framework, Role of the SIRO and Supporting Information Risk Management Infrastructure remain fit for purpose. In addition the Trust Board agrees the Registration Authority Lead Officer on the Trust Board as being Rod Barnes, Executive Director of Finance and Performance.		

RISK ASSESSMENT	Yes	No
Corporate Risk Register and/or Board Assurance Framework amended *If 'Yes' – expand in Section 4. / attached paper*	☐	☒
Resource Implications (Financial, Workforce, other - specify) *If 'Yes' – expand in Section 2. / attached paper*	☐	☒
Legal implications/Regulatory requirements If 'Yes' – expand in Section 2. / attached paper	☐	☒
Equality and Diversity Implications If 'Yes' – please attach to the back of this paper	☐	☒

ASSURANCE/COMPLIANCE	
Care Quality Commission **Choose a DOMAIN**	Not Applicable 21: Records
Monitor Quality Governance Framework **Choose a DOMAIN**	Not Applicable 1: Governance

1. PURPOSE/AIM

1.1 The purpose of this paper is to review the adequacy of the Information Governance Management Framework and ensure it remains fit for purpose.

1.2 In addition the purpose is to ensure the role and responsibilities of the Senior Information Risk Owner and supporting information risk management infrastructure i.e. Caldicott Guardian, Registration Authority Lead and Information Asset Owners, remain current, effective and correctly assigned.

2. BACKGROUND/CONTEXT

2.1 A number of Information Governance Toolkit requirements set out that the Trust should regularly review information governance arrangements to ensure they remain fit for purpose.

3. PROPOSALS/NEXT STEPS

3.1 The information governance arrangements for review are:

- **Requirement 12-101** *There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda*.
  Level 3a/b The adequacy of the Information Governance Management Framework is reviewed by the highest level of management on an annual basis to ensure it remains fit for purpose.

- **Requirement 12-200** *The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs.*
  Level 3b Policy and law change over time and it is important that the people assigned responsibilities for confidentiality and data protection remain updated and/or that the arrangements to access expertise are regularly reviewed.

- **Requirement 12-300** *The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs.*
  Level 3c Policy and law change over time as do technological advances. It is important that the people assigned responsibilities for information security remain updated and/or that the arrangements to access expertise are regularly reviewed.

- **Requirement 12-303** *There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority.*

Level 1a A member of the Board or equivalent, has been assigned (by the Board) overall responsibility for the RA function.

- **Requirement 12-307** *An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy.*
  Level 3a The role and responsibilities of the SIRO, and the supporting infrastructure are regularly reviewed to ensure that information risk management arrangements remain current and effective.

4. RISK ASSESSMENT

4.1 12-101 Adequacy of the information governance management framework remains fit for purpose.

The current information governance management framework (Appendix A) provides a summary of how the Trust is addressing the IG agenda. It describes all the areas required within IG Toolkit guidance; senior roles, key policies, key governance bodies, resources, governance framework.

In further support of the information governance management framework:

- An Information Governance Working Group meets quarterly.
- An information governance work programme is in place. IG related policy and IG related work programmes are approved by the Trust Management Group (TMG) and monitored by the Information Governance Working Group with the Clinical Governance Group (CGG) approving clinical elements of IG related work programmes as an adjunct to the TMG role.
- Information governance related incidents are monitored via the Incident Review Group and the Information Governance Working Group.
- The Risk and Assurance Group oversee the management of information governance risk.
- As part of the annual work plan East Coast Internal Audit are asked to assess the IG Toolkit processes and self-assessment by quarter 3 of the year.
- The Quality Committee receive regular assurance reports throughout the year on progress with information governance.
- The Audit Committee gains assurance on the adequacy of information governance risk via the annual internal audit of the Trusts IG Toolkit self-assessment.

4.2 12-200 People assigned responsibilities for confidentiality and data protection remain updated and the arrangements to access expertise are regularly reviewed.

- The key roles providing Information Governance expertise are detailed within the Information Governance Management Framework (Appendix A).
- Training requirements of key resources are detailed in Appendix D.

4.3 12-300 People assigned responsibilities for information security remain updated and the arrangements to access expertise are regularly reviewed.

- The key roles providing Information Governance expertise are detailed within the Information Governance Management Framework (Appendix A).
- Training requirements of key resources are detailed in Appendix D.

4.4 12-303 A member of the Board or equivalent, has been assigned (by the Board) overall responsibility for the RA function.

- A recommendation of this report is to agree the Registration Authority Lead Officer on the Trust Board as being Rod Barnes, Executive Director of Finance and Performance.

4.5 12-307 The role and responsibilities of the SIRO and the supporting infrastructure remain current and effective.

- Training requirements of key resources are detailed in Appendix D.
- The role and responsibilities of the SIRO is detailed in Appendix B and role and responsibilities of the IAO is detailed in Appendix C.

5. RECOMMENDATIONS

It is recommended that the Trust Board:-

1. Note the current arrangements and agree that the Information Governance Management Framework, role of the SIRO and supporting Information Risk Management Infrastructure remain fit for purpose.

2. In addition, the Trust Board agrees the Registration Authority Lead Officer on the Trust Board as being Rod Barnes, Executive Director of Finance and Performance.

6. APPENDICES/BACKGROUND INFORMATION

Appendix A

Yorkshire Ambulance Service NHS
NHS Trust
An Aspirant Foundation Trust

Information Governance Management Framework

Introduction and Purpose

The purpose of this framework is to summarise the management arrangements that deliver internal Information Governance assurance.

Accountabilities (who is responsible for leading and managing the information governance work programme)

Board Level Information Governance Function	**Name and Job title**
Senior Information Risk Owner (SIRO), Information Governance Lead, Information Security Lead	Steve Page, Executive Director of Standards and Compliance
Caldicott Guardian	Dr Julian Mark, Medical Director
Freedom of Information Lead	Ian Brandwood, Executive Director of People and Engagement
Registration Authority Lead	*Rod Barnes, Executive Director of Finance and Performance (to be agreed by the Trust Board)*

Resources (the key roles/functions involved in the information governance agenda below those at board level)

Resource	**Role/Function**
Data Protection Officer (primary link with ICO)	Acting Associate Director of ICT
Information Security Lead (ICT)	Acting Associate Director of ICT
Data Quality Lead	Head of Business Intelligence
Clinical Safety Officer (CSO)	Associate Director Risk and Safety
Information Governance	Information Governance Manager
Information Asset Owners	Departmental Heads/Heads of Service
Freedom of Information	Head of Engagement and Freedom of Information Administrator
Registration Authority	RA Manager, RA Advanced, RA Agents, RA Sponsors

IG Policies and Procedures (statement of intent and commitment relating to our policies)

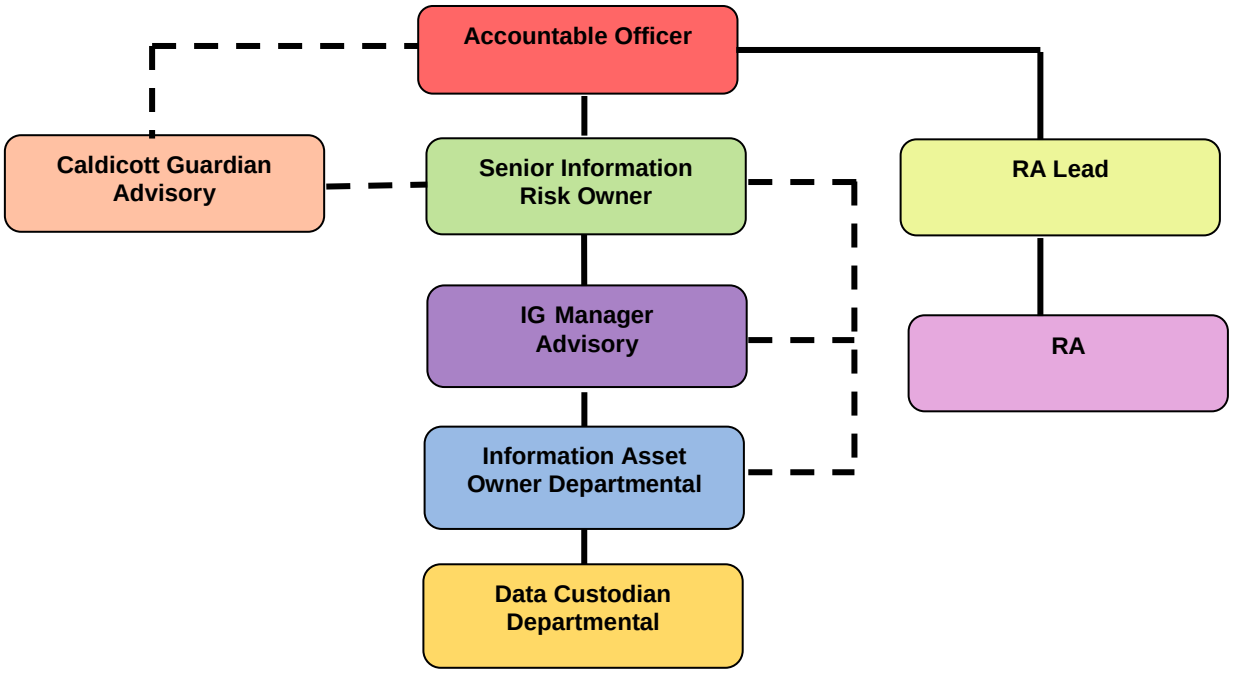
Policy Name	Review Date	Approval Body	Review Body
Data Protection Policy and Associated Procedures	November 2015	Trust Management Group	Information Governance Working Group
ICT Security Policy and Associated Procedures	February 2015	Trust Management Group	Information Governance Working Group
Internet Policy and Procedure	May 2015	Trust Management Group	Information Governance Working Group
Email Policy	May 2015	Trust Management Group	Information Governance Working Group
Records Management Policy	June 2015	Trust Management Group	Information Governance Working Group
Freedom of Information Policy (incorporating Environmental Information Regulations)	August 2016	Trust Management Group	Information Governance Working Group
Risk Management Procedures	January 2017	Trust Management Group	Incident Review Group
RA Policy and Associated Procedures	November 2016	Trust Management Group	Information Governance Working Group
Data Quality Policy	March 2016	Trust Management Group	Information Governance Working Group

Key Governance Bodies (forum/committees that regularly meet to deliberate on information governance issues)

Committee or Group	Function
Information Governance Working Group	To act as a forum for examining, co-ordinating and monitoring compliance to the Information Governance agenda; making recommendations to TMG, CGG, Quality Committee and the Board; creating and reviewing relevant policies and procedures and disseminating good practice on information governance as well as submitting an annual information governance self-assessment for external scrutiny.
Trust Management Group	To approve the annual Information Governance Work Programme, information governance relates policies and receive IG related issues for agreement/discussion.
Clinical Governance Group	To approve clinical elements of the Information Governance Work Programme as an adjunct to the TMG role.

Incident Review Group	To agree and monitor actions associated with information governance related incidents.
Risk and Assurance Group	To oversee the management of information governance risk.
Quality Committee	To monitor the organisations progress and compliance with information governance.
Audit Committee	To gain assurance on the adequacy of information governance risk via the annual internal audit of the Trusts IG Toolkit self-assessment.

Schematic Diagram of Information Governance Management Structure



Advisory - - - - - -

Reportable ———————

Governance Framework (details how responsibility and accountability for information governance is cascaded through the Trust)

Includes the following mechanisms:

- staff contracts,
- contracts with third parties that include appropriate information governance clauses,
- communications and awareness raising,
- information governance induction and mandatory training,
- identification of Information Asset Owners and asset owner responsibilities,
- risk assessments and sharing results of assessments and learning from incidents,
- independent audits.

Training and Guidance
Details of induction and mandatory training requirements are included in the Trusts Statutory and Mandatory Training Policy and Procedure.

Incident Management
Information Governance incidents are managed as per the Risk Management Procedures (which can be found on the Trusts intranet in the policies section).

Appendix B

Board Level Information Governance Functions *(extracts from Information Governance Toolkit)*

The Role of the Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) should be an Executive Director or other senior member of the Board (or equivalent senior management group/committee). The SIRO may also be the Chief Information Officer (CIO) if the latter is on the Board, but should not be the Caldicott Guardian as the SIRO should be part of the organisation's management hierarchy rather than being in an advisory role.

The SIRO will be expected to understand how the strategic business goals of the organisation may be impacted by information risks and it may therefore be logical for this role to be assigned to a Board member already leading on risk management or information governance.

The SIRO will act as an advocate for information risk on the Board and in internal discussions, and will provide written advice to the Accounting Officer on the content of the annual Statement of Internal Control (SIC) in regard to information risk.

The SIRO will provide an essential role in ensuring that identified information security risks are followed up and incidents managed and should have ownership of the Information Risk Policy and associated risk management Strategy and processes. He/she will provide leadership and guidance to a number of Information Asset Owners.

The key responsibilities of the SIRO are to:

- Oversee the development of an Information Risk Policy, and a strategy for implementing the policy within the existing Information Governance Framework.
- Take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control.
- Review and agree action in respect of identified information risks.
- Ensure that the organisation’s approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and/or discussion of information risk issues.
- Ensure the Board is adequately briefed on information risk issues.

Caldicott Guardian

The Guardian should be, in order of priority:

- an existing member of the senior management team;
- a senior health or social care professional;
- the person with responsibility for promoting clinical governance or equivalent functions.

The Guardian plays a key role in ensuring that the NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of an organisation, the 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.

The Caldicott Guardian also has a strategic role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework. This role is particularly important in relation to the implementation of national systems and the development of Electronic Social Care Records and Common Assessment Frameworks.

The Caldicott Guardian also needs to take into account the findings and recommendations from Dame Fiona Caldicott's second review of information governance in 2013 (the Caldicott2 Review). Importantly, the Review introduced a new Caldicott Principle to be used alongside the other six Principles when testing whether identifiable information should be used or disclosed.

Freedom of Information Lead

The Chief Executive (or equivalent) has the ultimate responsibility for their Public Authority's compliance with the Act and should ensure that responsibility for reporting Freedom of Information issues to the Board (or equivalent) is delegated to an appropriate Director (or equivalent) to act as Freedom of Information lead.

The senior management level lead should ensure organisational procedures and processes are in place to comply with the Act. The key responsibilities are to:

- ensure that the organisation complies with all aspects of the Act, associated Codes of Practice and related provisions in particular for contracting and procurement, minutes of meetings etc;
- provide reports to the Board (or equivalent) highlighting resource, performance and compliance issues;
- draft and / or maintain the currency of the organisation's policy;

- ensure that all staff are aware of their personal responsibilities for compliance with the Act and adhere to organisational policies and procedures;
- ensure training and written procedures are widely disseminated and available to all staff;
- ensure the general public has access to information about their rights under the Act;
- establish appropriate arrangements to deal with appeals and investigations into complaints about decisions and response times;
- liaise and work with other functions responsible for information handling activities, for example the Caldicott Guardian, data protection and information security staff;
- contribute to or liaise with external FOI networks or groups to keep updated on circular (round robin) requests.

Registration Authority (RA) Lead

There should be an Information Asset Owner assigned overall responsibility for the organisation's RA. This individual should also be a member of the Board to report to the organisation's Board on RA matters in person.

To ensure adequate governance, senior members of staff and appropriate areas of the organisation should also be involved, such as the Senior Information Risk Owner, the Caldicott Guardian, Human Resources Director, Clinical Directors and the IM&T Director.

The RA Manager and Sponsor roles need to be assigned to trusted individuals and formally recorded by the local Executive Management Team.

The responsibilities of an RA Manager are to assign, sponsor and register RA agents and assist Sponsors in understanding Role Based Access Control (RBAC) and Position Based Access Control (PBAC), by the development of access control positions, and in finding information about applications they sponsor Users for.

The RA Manager is also responsible in developing and updating the organisation's RA policy and processes ensuring that is aligned to the National RA policy and processes.

Appendix C

Information Asset Owners 2014/15

Directorate/Department	Information Asset Owners
Business Intelligence	Business Intelligence Manager
Clinical Directorate	Associate Medical Director
Corporate Communications	Head of Corporate Communications
EOC	*Currently under review*
Estates	Estates Manager
Fleet	Head Of Fleet Services
Finance	Financial Controller
Human Resources	Head of HR Policy and Business Services
ICT	Acting Associate Director of ICT
Legal Service	Senior Legal Services Coordinator
Membership Programme	Foundation Trust Membership Officer
NHS 111	Head of Quality Assurance, NHS 111 and Head of Service Delivery NHS 111
Operational Resource	Head of Operational Resource Planning
Operations	*Currently under review*
Patient Services	Patient Relations Manager
Procurement	Interim Head of Procurement
PTS and Comms	Associate Director of Operations PTS (Planning and Strategy)
Risk and Quality	Head of Safety
Safeguarding	Head of Quality and Patient Experience

The Role of the Information Asset Owner (IAO)

1. Overview and Background

The Information Asset Owner (IAO) will be a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. It is a core IG objective that all Information Assets of the organisation are identified and that the business importance of those assets is established.

There may be several IAOs within an NHS organisation, whose departmental roles may differ. IAOs will work closely with other IAOs of the organisation to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. This is especially important where information assets are shared by multiple parts of the organisation.

2. Accountability and Performance

IAOs will support the organisation's SIRO in their overall information risk management function as defined in the organisation's policy**.**

3. JOB SUMMARY

3.1. **Policy and process**

- Identify and document the scope and importance of all Information Assets they own. This will include identifying all information necessary in order to respond to incidents or recover from a disaster affecting the Information Asset.
- Take ownership of their local asset control, risk assessment and management processes for the information assets they own. This includes the identification, review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks.
- Provide support to the organisation's SIRO and Risk Management Board to maintain their awareness of the risks to all Information Assets that are owned by the organisation and for the organisation's overall risk reporting requirements and procedures.
- Ensure that staff and relevant others are aware of and comply with expected IG working practices for the effective use of owned Information Assets. This includes records of the information disclosed from an asset where this is permitted.
- Ensure that adequate data quality assurances are in place an that all assets are risk assessed for data quality.
- Lead on Information Quality and records management for their respective areas.
- Provide a focal point for the resolution and/or discussion of risk issues affecting their Information Assets.

3.2. **Incident Management**

- Ensure that the organisation's requirements for information incident identification, reporting, management and response apply to the Information Assets they own. This includes the mechanisms to identify and minimise the severity of an incident and the points at which assistance or escalation may be required.

3.3 **Leadership**

- Foster an effective IG culture for staff and others who access or use their Information Assets to ensure individual responsibilities are understood, and that good working practices are adopted in accordance with the organisation's policy.

KEY RELATIONSHIPS

Within the Organisation:

- SIRO
- Corporate Services
- IG Lead
- Risk Managers
- Information Security Manager
- Other Information Asset Owners
- Records Manager
- Caldicott Guardian (for assets that process patient data)
- Users of the Information Assets they own

May have contact with:

- Other NHS Organisations and external business partner

Appendix D - Training Requirements of Key Resources 14/15

Staff Group	Level	Training Objective/Aim	Module/Course Name	Method of Delivery	Frequency of Training	Completed
Senior Information Risk Owner (SIRO)	Expert Level	An introductory module that describes key responsibilities for the SIRO and IAO roles, and outlines the structures required within organisations to support those staff with SIRO or IAO duties.	NHS Information Risk Management for SIROs and IAOs.	IG Training Tool (e-learning)	Yearly	Completed
Caldicott Guardian	Expert level	A practitioner level module aimed at newly appointed Caldicott Guardians and those needing to know more about the role of the Caldicott Guardian.	The Caldicott Guardian in the NHS and Social Care.	IG Training Tool (e-learning)	Once only	Completed
Information Asset Owners (IAOs)	Expert Level	An introductory and foundation level module intended to assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties. An introductory module that describes key responsibilities for the SIRO and IAO roles.	NHS Information Risk Management Introduction, NHS Information Risk Management Foundation and NHS Information Risk Management for SIROs and IAOs.	IG Training Tool (e-learning)	Once only	Completion is monitored via the quarterly IAO review meetings as there have been a number of changes to IAOs in this year.
Information Asset Owners (IAOs)	Essen-tial Level	Refresher/update on the role of the IAO and delivery of specific topics related to the role of the IAO.	In house IAO Workshop.	Classroom (Workshop)	Twice yearly	Signing in sheet taken. Not all members have attended the sessions held to date.
Information Governance Manager	Expert Level	In-depth understanding of the Data Protection Act 1998 (and associated legislation) and Freedom of Information Act 2000 and Environmental Information Regulations, information security.	Information Security Exam Board (ISEB) Data Protection, Freedom of Information as well as regular updates at local/ national events.	Specialist Courses and examinations	Once only	Completed
Information Security Lead (ICT)	Expert Level	Professional certification in one or more information security competencies.	Certified Information Systems Security Professional (CISSP) and Certificate in Information Security Management Principles BCS.	Specialist Courses and examinations	Once only	Completed both courses (ICT are currently assessing arrangement for access to technical information security expertise).