NHS
Yorkshire
Ambulance Service
NHS Trust

Information Governance Policy

Document Author: Information Governance Manager

Date Approved: May 2018

Document Reference	PO – Information Governance Policy
Version	V8.2
Responsible Committee	Trust Management Group
Responsible Director	Executive Director Quality, Governance and Performance Assurance, SIRO
Document Author	Information Governance Manager
Approved By	Trust Management Group
Date Approved	May 2018
Review Date	March 2021
Equality Impact Assessed (EIA)	Yes – Screening
Protective Marking	Not protectively marked

Document Control Information

Version	Date	Author	Status	Description of Change
1.0	Mar 2007	David Johnson	A	Approved and ratified by Information Governance Group
2.0	Dec 2011	David Johnson	A	Approved and ratified by Information Governance Group
3.0	Nov 2012	Caroline Squires	A	Includes minor amendments following approval by Senior Management Group
4.0	6 Nov 2013	Caroline Squires	A	Approved SMG
5.0	Oct 2014	Caroline Squires	A	Approved TMG. Updates to the Information Governance Management Framework within Appendix C and updates to Appendix D, E and H. Minor changes to format of the policy.
5.1	Nov 2014	Caroline Squires	A	Minor amendment to Caldicott Guardian role description under Appendix B.
5.2	Oct 2015	Caroline Squires	D	Minor accuracy updates throughout.
6.0	Nov 2015	Caroline Squires	A	Approved by TMG
6.1	Dec 2016	Leon Kaplan	D	Minor accuracy updates
7.0	Feb 17	Leon Kaplan	A	Approved by TMG
7.1	March 17	Maxine Travis	A	Updated dates on reviewed policies in Appendix C IG Management Framework
7.2	May 2018	Allan Darby	A	Extension agreed at TMG in preparedness for the launch of General Data Protection Regulations which come in to force May 2018. IG policies remain best practice up to this date.
7.3	Apr 2018	Allan Darby	D	Amended to reflect GDPR and Data Security and Protection Toolkit requirements.
7.4	April 2018	Risk Team	D	Document formatted – New Visual Identity
8.0	May 2018	Risk Team	A	Approved at TMG
8.1	March 2019	Risk Team	D	Updated list of associated policies pg.14
8.2	August 2020	Ruth Parker	D	Date agreed by TMG for review date extension
A = Approved D = Draft				

Document Author = Information Governance Manager
Associated Documentation: Information Governance Strategy Data Protection Policy and Associated Procedures Internet Policy and Procedure Email Policy ICT Security Policy and Associated Procedures Records Management Policy Safety and Security Policy YAS Code of Conduct Disciplinary Policy and Procedure Management of Online and Digital Services Procedure Social Media Policy Freedom of Information Policy

Staff Summary

The purpose of this policy is to inform all Trust staff of their responsibility for ensuring that corporate, patient and personal information is safeguarded and used appropriately within the Trust.
Information Governance is a framework for handling information in a confidential and secure manner to appropriate ethical and quality standards.
The Information Governance Management Framework (Appendix C) sets out the resources to deliver Information Governance.
There are five key strands to the Information Governance Policy; Openness, Legal Compliance, Information Security, Quality Assurance and Information Governance Management and Accountability.
The Trust regards all identifiable personal information relating to patients as confidential.
Non-confidential information about the Trust and its services should be available to the public through a variety of media, in line with the Trust's code of openness.
The Senior Information Risk Owner (SIRO) is responsible for the Trust's information risk and acts as advocate for information risk on the Trust Board. The Trust's Senior Information Risk Owner is the Executive Director of Quality, Governance and Performance Assurance.
Information Asset Owners are responsible for interpreting information governance policy, applying it on a practical level within their area of responsibility and ensuring that policies and procedures are followed by staff.
Staff should refer any questions about this policy to their Information Asset Owner or line manager.

1.0 Introduction

1.1 Yorkshire Ambulance Service NHS Trust recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources.

1.2 Information governance plays a key part in supporting clinical governance, service planning and performance management. It also gives assurance to Yorkshire Ambulance Service NHS Trust and to individuals that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care and to meet Yorkshire Ambulance Service NHS Trust's legal and good practice responsibilities.

1.3 Yorkshire Ambulance Service NHS Trust will establish and maintain policies and procedures to ensure compliance with legal requirements and the requirements contained in the Data Security and Protection (DSP) Toolkit, managed by NHS Digital.

1.4 This policy should be read in conjunction with the Trust's Information Governance Strategy.

2.0 Purpose/Scope

2.1 The purpose of this policy is to inform all Trust staff of their responsibility for ensuring that corporate, patient and personal information is safeguarded and used appropriately within the Trust. It covers all aspects of information within the Trust including:

- Patient information (Person Confidential Data)
- Staff information
- Organisational information

2.2 All aspects of handling information are covered by this policy, including paper and electronic structured record systems and the transmission of information via mail, e-mail, fax and telephone.

2.3 This policy covers all systems utilised by Yorkshire Ambulance Service NHS Trust and any individual employed, in any capacity, by the Trust or working in a voluntary capacity.

3.0 Policy Statements

3.1 Principles

3.1.1 The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

3.1.2 The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard personal information about patients, staff and commercially sensitive information.

3.1.3 The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and in some circumstances, the interests of the public.

3.1.4 The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

3.1.5 There are five key strands to the Information Governance Policy:

- Openness
- Legal compliance
- Information security
- Quality assurance
- Information Governance management and accountability

3.2 Openness

3.2.1 Non-confidential information about the Trust and its services should be available to the public through a variety of media, in line with the Trust's code of openness.

3.2.2 The Trust continues to establish and maintain procedures to ensure compliance with the Freedom of Information Act.

3.2.3 The Trust continues to undertake or commission annual assessments and audits of its policies and arrangements for openness.

3.2.4 Patients have ready access to information relating to their own health care, including information about complications, errors and near miss events, their options for treatment and their rights as patients.

3.2.5 The Trust has clear procedures and arrangements for liaison with the press and the broadcasting media.

3.2.6 The Trust has clear procedures and arrangements for handling queries from patients and the public.

3.3 Legal Compliance

3.3.1 The Trust ensures that patients are made aware that the information they give may be recorded or shared in order to provide them with care, and may be used to support local clinical audit and other work to monitor the quality of care provided.

3.3.2 The Trust regards all identifiable personal information relating to patients as confidential. The Trust's approach to the monitoring and auditing of access to confidential personal information is set out in this policy.

3.3.3 The Trust undertakes or commissions annual assessments and audits of its compliance with legal requirements.

3.3.4 The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

3.3.5 The Trust has established and maintains policies to ensure compliance with the Freedom of Information Act 2000, the General Data Protection Regulations (GDPR) 2016, Data Protection Act (DPA) 2018 and other relevant legislation relating to the security and use of both personal and non-personal information.

3.3.6 The Trust ensures that non-personal, non-confidential information is available through a variety of media in line with the Trust's Freedom of Information Publication Scheme and Freedom of Information procedures.

3.3.7 The Trust has established and will maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. The Health and Social Care (Safety and Quality) Act 2015, Crime and Disorder Act 1998, Protection of Children Act 1999).

3.3.8 The Trust will ensure that any transfers of personal information outside of the European Economic Area are only carried out when sufficient security exists within the receiving country and the requirements of the GDPR and DPA have been met.

3.4 Information Security

3.4.1 The Trust has established and will maintain policies for the effective and secure management of its information assets and resources.

3.4.2 The Trust undertakes or commissions annual assessments and audits of its information and IT security arrangements.

3.4.3 The Trust promotes effective confidentiality and security practice to its staff through policies, procedures and training.

3.4.4 The Trust has established and will maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

3.4.5 The Trust has established and will maintain appropriate policies and procedures for the disposal of paper based material that contains confidential information and for the disposal of electronic storage devices (e.g. redundant hard drives). Processes specifically ensure that electronic storage devices carrying confidential information, or which may have done so in the past, are securely over-written or physically destroyed.

3.4.6 The Trust will establish and maintain formal policies and procedures for the secure management of documents containing confidential information (such as patient or personnel records), when all or part of a building is vacated by the Trust.

3.5 Information Quality Assurance

3.5.1 The Trust has established and maintains policies for information quality assurance and the effective management of its clinical and non-clinical records.

3.5.2 The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements.

3.5.3 Managers are expected to take ownership of, and seek to improve the quality of information within their services.

3.5.4 Wherever possible, information quality should be assured at the point of collection.

3.5.5 Data standards are set through clear and consistent definition of data items, in accordance with national standards.

3.4.6 The Trust promotes information quality and effective records management through policies, procedures/ user manuals and training.

4.0 Training expectations for staff

4.1 Training is delivered as specified within the Trust Training Needs Analysis (TNA).

5.0 Implementation Plan

5.1 The latest approved version of this policy will be posted on the Trust Intranet site for all members of staff to view. New members of staff will be signposted to how to find and access this policy and associated procedures during Trust Induction.

6.0 Monitoring Compliance with this Policy

6.1 To be assured that this policy is being implemented, key elements will be monitored for compliance.

- **Compliance against all 10 Data Security Standards of the ambulance trusts DSP Toolkit.** The Quality Committee will monitor overall progress through receipt of quarterly reports. The Information Governance Working Group will monitor operational progress throughout the year and take action to address any concerns and deficiencies will be noted and reviewed at subsequent meetings. Individual DSP Toolkit 'standard' leads will additionally monitor operational progress throughout the year against specific action plans.

- **All staff receive annual training and competency test in information governance.** The Quality Committee will monitor progress through receipt of quarterly Information Governance reports.

- **All Information Asset Owners (IAOs) trained in their role and undertaking quarterly risk reviews of information assets they are responsible for. New information assets will be identified through this quarterly review process.**
  Quality Committee will monitor progress through receipt of quarterly Information Governance reports. The Information Governance Working Group will monitor operational progress throughout the year and take action to address any concerns and deficiencies will be noted and reviewed at subsequent meetings.

- **Statistically validated reduction in Information Governance related incidents.** Monitoring of incidents by both the Clinical Governance Group (Caldicott Log) and through the Information Governance Working Group.

- **No Data Protection Act undertakings, enforcement notices or 'stop now' orders, compulsory assessment notices or monetary penalty notices served on the organisation. No Freedom of Information Act enforcement notices served on the organisation.** The Trust Board and Quality Committee will monitor progress through receipt of quarterly Information Governance reports.

- **Staff know who and where to direct information governance concerns and queries to.** Results of IG staff survey presented to the IG Working Group.

7.0 References

- Great Britain. 2018. Data Protection Act 2018. London: HMSO. Available at: www.legislation.gov.uk
- European Union. 2016. EU General Data Protection Regulations 2016. Available at: www.eugdpr.org
- Great Britain. 2000. Freedom of Information Act 2000. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2004. *Environmental Information Regulations 2004.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Computer Misuse Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Access to Health Records Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1958 and 1967. *Public Records Act 1958 and 1967.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. *Crime and Disorder Act 1998*. *Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2000. *Electronic Communications Act 2000.* London: HMSO. Available at: www.legislation.gov.uk
- Department of Health, 2000. Publications: Information Governance Toolkit. Available at: https://nww.igt.hscic.gov.uk/
- Department of Health, 2003, Publications: *Confidentiality NHS Code of Practice* Available at: www.dh.gov.uk
- Information Governance Alliance, 2016, Publications: *Records Management Code of Practice for Health and Social Care.* Available at: https://digital.nhs.uk/article/402/Information-Governance

8.0 Appendices

Appendix A Definitions

The definitions or explanation of terms relating to this policy are:-

Data (information) sharing	The disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. This can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose or for exceptional, one-off decisions to share data for any of a range of purposes.
Information Governance	The set of multidisciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements.
Data Security and Protection Toolkit	The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.
Personal Confidential Data (PCD):	Personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this Review 'Personal' includes the DPA definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.
Personal data	Data which relate to a living individual who can be identified from those data, or from those data and other information which are in the possession of, or are likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Appendix B Roles & Responsibilities

There is a robust management structure that underpins and supports this policy. In line with the requirements of the Data Security and Protection Toolkit, a more extensive summary of the resources and management arrangements that deliver internal information governance assurance is detailed in the Information Governance Management Framework at Appendix C.

Chief Executive
As the accountable officer for the Trust, the Chief Executive is required to provide assurance that all risks to the Trust (including information risks) are effectively identified, managed and mitigated.

Trust Management Group (TMG)
The Trust Management Group consists of Executive Directors and Associate Directors and is chaired by the Chief Executive. The Group carries delegated responsibility from the Trust Executive Group for approving this policy.

Information Governance Working Group
The Information Governance Working Group, which consists of all information Asset Owners.

Senior Information Risk Owner
A Board-level Senior Information Risk Owner (SIRO) will be responsible for the Trust's information risk and act as advocate for information risk on the Trust Board. The Trust's Senior Information Risk Owner is the Executive Director of Quality, Governance and Performance Assurance.

A more detailed description of the SIRO role can be found in Appendix F.

Caldicott Guardian
The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian is responsible for providing advice within the Trust on the lawful and ethical processing of patient information. The Executive Medical Director acts as the Trust's Caldicott Guardian and is supported on a day to day basis by the Deputy Medical Director who plays a key role in ensuring that the organisation satisfies the highest practicable standards for handling patient identifiable information.

Data Protection Officer
A Data Protection Officer (DPO) is a role mandated for public bodies, for organisations carrying out regular and systematic monitoring of data subjects on a large scale, and for organisations carrying out large scale processing of special categories (e.g. health and social care) data or criminal convictions data. The Head of Legal Services acts as the Trust's DPO and is supported on a day to day basis by the IG Manager and Legal Services Manager. The DPO advises the organisation on data protection matters, monitors compliance and is a point of contact on data protection for the public and the ICO.

Information Asset Owners
The SIRO is supported by a network of Information Asset Owners and Information Asset Administrators. These individuals are responsible for interpreting information governance policy, applying it on a practical level within their area of responsibility and ensuring that policies and procedures are followed by staff. They recognise actual or potential security incidents, consult with the SIRO and Caldicott Guardian in relation to incident management and ensure that information asset registers are accurate and up to date.

A more detailed description of the Information Asset Owner role can be found in the appendices.

Information Governance Manager
The Information Governance Manager provides day-to-day operational support to the SIRO and Caldicott Guardian.

Other roles work closely to support the information governance agenda and include the following: Data Protection Officer, Information Security Officer, Freedom of Information Officer, Corporate and Clinical Governance leads, RA Lead, RA Manager, RA Agents and Sponsors.

Line Managers
All line managers are responsible for ensuring that all employees are aware of this and related policies.

All Staff
All staff must read and understand this policy as well as related policies and procedures and refer any questions to the department's Information Asset Owner or line manager.

Appendix C

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 Quality, Governance and Performance Assurance, Deputy Chief Executive
Caldicott Guardian	Dr Julian Mark, Executive Medical Director
Freedom of Information Lead	Head of Legal Services and Trust Solicitor
Registration Authority Lead	Mark Bradley, Executive Director of Finance

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)	Head of Legal Services and Trust Solicitor
Information Security Lead (ICT)	Head of ICT
Data Quality Lead	Head of Business Intelligence
Clinical Safety Officer (CSO)	Deputy Director of Quality and Nursing
Information Governance	Information Governance Manager
Information Asset Owners	Departmental Heads/Heads of Service
Freedom of Information	Head of Legal Services and Trust Solicitor; Freedom of Information and Stakeholder Engagement Administrator
Registration Authority	RA Manager, RA Advanced, RA Agents, RA Sponsors

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

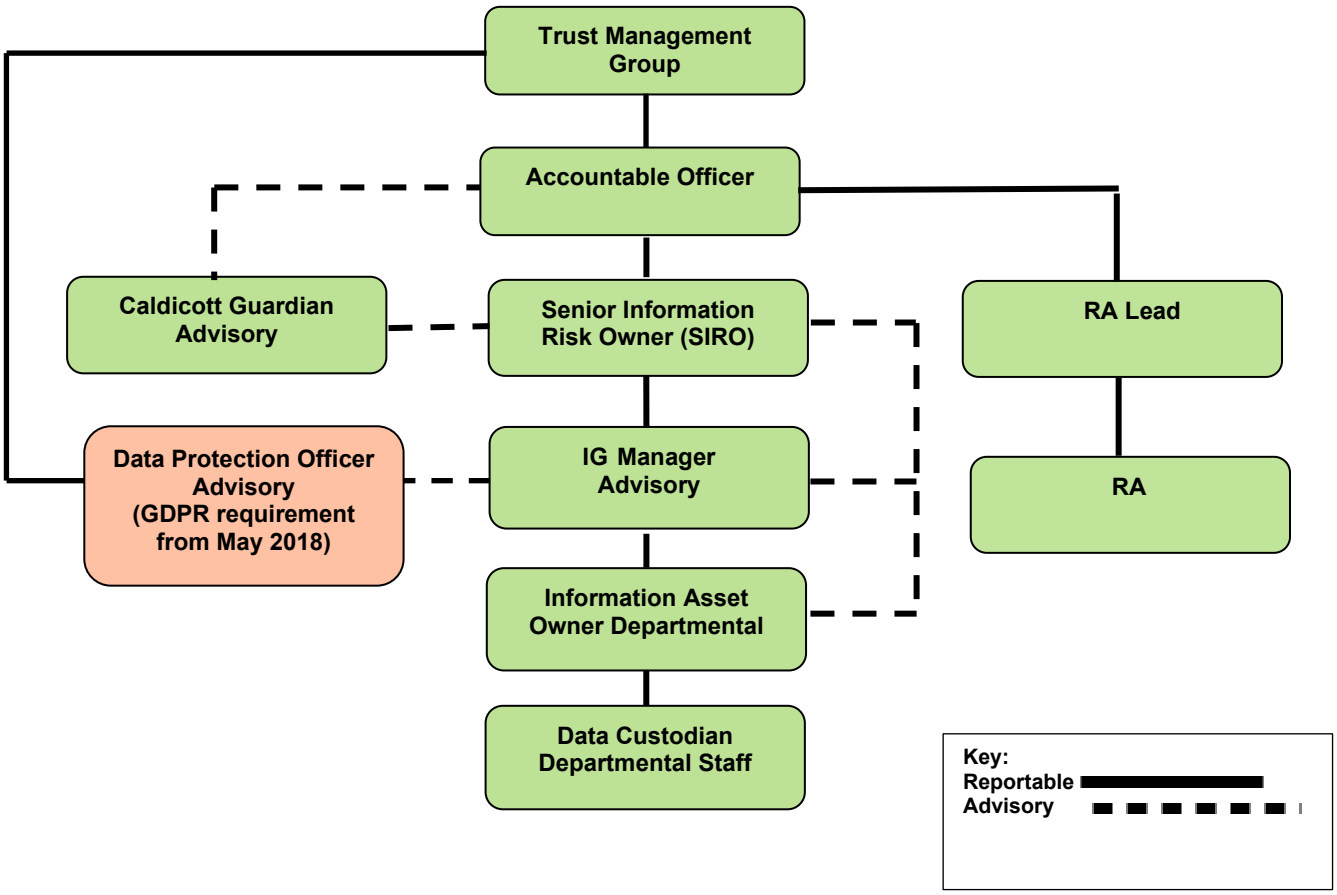
Policy Name	Review Date	Approval Body	Review Body
Data Protection Policy and Associated Procedures	May 2020	Trust Management Group	Information Governance Working Group
ICT Security Policy and Associated Procedures	February 2020	Trust Management Group	Information Governance Working Group
Internet Policy and Procedure	November 2019	Trust Management Group	Information Governance Working Group
Email Policy	June 2019	Trust Management Group	Information Governance Working Group
Records Management Policy	May 2020	Trust Management Group	Information Governance Working Group
Freedom of Information Policy (incorporating Environmental Information Regulations)	March 2019	Trust Management Group	Information Governance Working Group
Investigations and Learning Policy	June 2020	Trust Management Group	Incident Review Group
RA Policy and Associated Procedures	August 2020	Trust Management Group	Information Governance Working Group
Data Quality Policy	June 2018	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, Clincial Quality Development Forum (and where necessary to the Clinical Quality Group), 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.

Committee or Group	Function
Trust Management Group	To approve the annual Information Governance Work Programme, information governance related 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.
Clinical Quality Development Forum	To provide the first drafts of papers for CCG, meet regularly, and identify and monitor clinical treatment options more refinely.
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 DSP Toolkit self-assessment.

Schematic Diagram of Information Governance Management Structure



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 and which are reviewed on a regular basis to ensure they remain effective and meet the evolving IG agenda,
- 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 of the Trust's information governance arrangements including reviews and/or audits to obtain assurance that all third parties that have access to the organisation's information assets are complying with contractual IG requirements.

Training and Guidance
Details of induction and mandatory training requirements are included in the Trust's 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 Trust's intranet in the policies section).

Appendix D Information Governance Communication Plan

Internal/ External Communication	Activity	Frequency	Responsibility
External Communication	▪ Patient Information Poster ” Keeping Patients Informed - How we use your personal information” to be made available on notice boards in public facing operational areas	Reviewed at site visits	Information Governance Manager
	▪ Initial point of contact for queries in relation to the poster (*as already set out on the poster*)	Ongoing activity	Patient Relations Department
External Communication	**Information leaflets relating to specific initiatives relating to the use of patient information** ▪ Specific leaflets on the advice of the Caldicott Guardian/SIRO/DPO/Information Governance Manager	As and when required	Caldicott Guardian /SIRO /DPO/ Information Governance Manager
External Communication	**Public Website** ▪ Information on how the Trust may use patients information (to meet fair processing obligations as set out by the General Data Protection Regulations and Data Protection Act 2018)	Reviewed yearly	Corporate Communications /Information Governance Manager
	▪ Initial point of contact in relation to queries (*as per the web site content)*	Ongoing activity	Patient Relations Department
Internal Communication	**Staff Update** ▪ Reinforcing and repeating key IG messages to reach the majority of staff and communicate a basic brief. To raise awareness of an important area of information governance in more detail including information security, data protection, confidentiality, Caldicott, records management, Freedom of Information and NHS Smartcard usage responsibilities in line with the Terms and Conditions of Smartcard use.	Bi annually	SIRO/Caldicott Guardian/DPO/ Information Governance Manager

Internal Communication	**Training –** ▪ All Trust staff require IG Training as per the Data Security and Protection Toolkit – Standard 3. Topics include information security, data protection, confidentiality, Caldicott, records management, Freedom of Information and NHS Smartcard usage responsibilities in line with the Terms and Conditions of Smartcard use. .	Ongoing activity monitored through IPR	SIRO/Information Governance Manager
Internal Communication	**Staff Handbooks –** ▪ Provision of key IG messages in the Trusts "Staff Handbook". Review of staff handbook in relation to information governance content	Reviewed yearly	Information Governance Manager/ Organisational Effectiveness and Education
	▪ Additional leaflets to be created and distributed to all staff, raising the awareness of the importance of information governance and handling information securely and efficiently. Leaflets to contain contact details for specific queries	As and when required	Information Governance Manager/relevant DSP Toolkit standard lead officer
Internal Communication	**Intranet –** ***Primary source for information and news across the Trust***		
	▪ Include updated policies, procedures, presentations, guidance, training, information.	Ongoing activity	DPO/Information Governance Manager/Risk and Safety Team
	▪ Information Governance reference pages on the Trust intranet	Reviewed yearly	Information Governance Manager

Acknowledgements: The Health Informatics Service

Appendix E

Yorkshire Ambulance Service NHS
NHS Trust
An Aspirant Foundation Trust

Confidentiality Audit Procedures

Document Reference	PR - Confidentiality Audit Procedures
Version	V4
Document Author	Information Governance Manager
Approved By	Trust Management Group
Date Approved	May 2018
Review Date	May 2020

1.0 Introduction

1.1 In order to provide assurance that access to confidential person identifiable information is gained only by those individuals that have a legitimate right of access to the information, the Trust ensures that access to person identifiable information is monitored on a regular basis.

1.2 For the purposes of this procedure, confidential person identifiable information is defined as any information about a person which would allow that person to be identified.

1.3 With advances in the electronic management of both health and employment information within the NHS brought about by the advent of the NHS Care Record Service and Electronic Staff Record for example, the requirement to monitor access to confidential person identifiable information has become increasingly important. With the large number of staff using these systems, it is imperative that access is strictly monitored and controlled.

1.4 In relation to electronic, as well as paper based patient and staff records, failure to ensure that adequate controls to manage and safeguard confidentiality are implemented, may result in a breach of confidentiality. This would contravene the requirements of Caldicott, the General Data Protection Regulations 2016, the Data Protection Act 2018, the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

1.5 Unauthorised access to confidential information by any individual will be considered against the Trust's disciplinary procedures. Any breaches of confidentiality or security made outside the proper course of duty may be treated as a serious disciplinary offence which could lead to dismissal from employment.

2.0 Process

2.1 The following table (Table 1) details the organisations current approach to auditing confidential personal identifiable information, and makes provision for assurances around paper based records as well as electronic records.

2.2 The organisations Information Asset Owners are responsible for ensuring that confidentiality audits are implemented throughout the Trust and for ensuring that access to electronic and manual confidential information is strictly controlled within their area and in relation to specific information assets.

2.3 All staff are responsible for complying with confidentiality audits conducted within their area. All staff are additionally responsible for complying with recommendations which are made as a result of such audits.

2.4 The audit and monitoring programme detailed in Table 1 will be carried out in an open and transparent manner. These procedures will be available on the Trust intranet and the Staff Update bulletin will be used to communicate the programme to staff.

2.5 If you have any questions about confidentiality audits, please contact the Information Governance Manager via the ICT Service Desk on 0300 3305417.

3.0 Monitoring Compliance with this Procedure

3.1 Table 1 details the monitoring and reporting approach that will be taken in relation to each audit activity type.

4.0 References

- NHS Digital: Data Security and Protection Toolkit. Available at: www.dsptoolkit.nhs.uk/
-

Table 1

Approach to Confidentiality Audit

Objective of Audit	Audit (or monitoring) Approach	Responsible Officer	Frequency of Audit	Audit Tool	Reporting of Findings
To ensure confidentiality and information security compliance in relation to access to the organisation's confidential information assets	Applies to all departmental areas Unannounced compliance checks covering the following areas: information security, data protection, confidentiality, Caldicott and NHS Smartcard usage responsibilities in line with the Terms and Conditions of Smartcard use.	Information Asset Owners Inspection for Improvement organisation leads	Annually	Locally developed Audit Tool Key questions within the Inspection for Improvement visits	IAO / Information Governance Working Group
To ensure appropriate use of electronic systems and associated records, to cover as a minimum: 1. checks that access to assets by staff who have left the organisation or changed role, has been revoked, and 2. checks for multiple log-on attempts and lock-outs	Applies to all electronic information assets holding person identifiable information Checks to ensure access to systems have been revoked Use of audit trail functionality	Information Asset Owners	Quarterly	Locally developed Audit Tool	IAO / Information Governance Working Group
To ensure standards and processes are being adhered to in relation to corporate records management	Planned audit of at least 4 departmental areas	Information Asset Owners and Information Governance Manager	Annually	Audit Tool (based on IGA tools)	Information Governance Working Group

Objective of Audit	Audit (or monitoring) Approach	Responsible Officer	Frequency of Audit	Audit Tool	Reporting of Results
To ensure high levels of awareness in relation to Information Governance arrangements across the whole organisation	Random Questionnaire Survey	Information Governance Manager	Annually	Locally developed Questionnaire	Information Governance Working Group
To monitor reports of actual or potential access to confidential person identifiable information e.g. Lost PRF forms, verbal disclosures, stolen/lost laptops, lost Smartcards.	On-going scrutiny of patterns and trends and lessons that can be learnt from incidents	Caldicott Guardian and Information Governance Manager	Continuous Activity	Caldicott Log presented to Clinical Quality Development Forum Integrated Information Governance Report presented to Information Governance Working Group	Information Governance Working Group/CDQF

Reporting of Results and Taking Action

Once the audit has been completed a brief report should be produced by the auditor detailing the outcome of the audit. It should include a summary of the findings of the audit, together with observations of non-compliance and recommendations which have been made. This should be presented to the Information Asset Owner. Whilst the Information Asset Owner Quarterly Information Risk Review Meetings with the Information Governance Manager will be used to go through the findings of audits and agree the corrective actions if required, Information Asset Owners are responsible for ensuring areas of none compliance and recommendations are actioned at the earliest opportunity out with these meetings and that risks are reflected on risk registers.
If there are any suspicious findings from Audit Trail results these must be immediately reported to the SIRO and/or the Caldicott Guardian who will decide if further investigations should be carried out or disciplinary action taken.
Information Asset Owners should contact the Information Governance Manager for support and advice as and when required.

Appendix F The Role of the Senior Information Risk Owner (SIRO)

1. Overview and Background

The SIRO is concerned with identifying and managing the information risks to the organisation and with its business partners. This will include oversight of the organisation's information security incident reporting and response arrangements. The SIRO will be supported by one or more information asset owners who have assigned responsibility for the information assets of the organisation

The establishment of the role of SIRO is one of several measures to strengthen controls around information security. The SIRO should be an Executive or Senior Manager on the Board who is familiar with information risks and the organisation's response to risk and has the knowledge and skills necessary to provide the required input and support to the Board and to the Chief Executive.

2. Accountability and Performance

Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of YAS. Senior leadership demonstrates the importance of the issue and is critical in obtaining the resources and commitment necessary to ensuring information security remains high on the Board agenda.

3. The role of the Accountable Officer

The Chief Executive, as Accountable Officer of the Trust, has overall accountability and responsibility for Information Governance in the organisation and is required to provide assurance, through the Statement of Coolpiance (SOC), that all risks to the Trust, including those relating to information, are effectively managed and mitigated.

4. The role of the Senior Information Risk Officer (SIRO)

The SIRO will be an Executive Director, Chief Information Officer or Senior Manager member of the Board. The SIRO may also be the Chief Information Officer if the latter is on the Board.
The SIRO will be expected to understand YAS's strategic business goals and how this may be impacted by information risks.

The SIRO will act as an advocate for information risk on the Board and in internal discussions, and will provide written advice to the Chief Executive on the content of their annual Statement of Internal Control in regard to information risk.

Working within a simple governance structure, with clear lines of ownership and well defined roles and responsibilities, the SIRO will provide an essential role in ensuring the identified information security threats are followed up and incidents managed. They will also ensure that the Board and the Accountable Officer are kept up-to-date on all information risk issues. The role will be supported by the Trust's Information Governance Manager, the Trust's Risk Manager, the Trust's Information Security Manager and the Trust's Caldicott Guardian, although ownership of the Information Risk Policy and risk assessment process will remain with the SIRO.

5. Key responsibilities of the SIRO

To oversee the development of an Information Risk Policy and a strategy for implementing the policy within the existing Information Governance Framework.

Appendix G

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 and 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
- Data Protection Officer
- 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 H Information Asset Owners

Directorate/Department	Information Asset Owners
Business Intelligence	Head of Business Intelligence
Clinical Directorate	Deputy Medical Director
Corporate Communications	Head of Corporate Communications
EOC	Locality Director EOC
Estates	Estates Manager
Fleet	Fleet Services Administration Manager
Finance	Head of Financial Services
Human Resources	Head of HR Operations
ICT	Associate Director of ICT
Legal Service	Legal Services Manager
Membership Programme	Community Engagement Manager
NHS 111	Head of Nursing and Quality Assurance, NHS 111
Operational Resource	Head of Operational Resource Planning
Operations	Service Planning and Development Manager
Patient Services	Patient Relations Manager
Procurement	Associate Director of Procurement and Logistics
PTS and Comms	PTS Operations systems manager
Quality and Safety	Head of Safety
Risk	Head of Risk – Chair IGWG
Safeguarding	Head of Safeguarding