East of England Ambulance Service NHS Trust

Information Governance Strategy

Document Reference	POL010
Document Status	Approved
Version:	V6.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author**
Information Governance Requirements	September 2007	Information Governance Group
Version	**Date**	**Comments (i.e. viewed, or reviewed, amended approved by person or committee)**
V0.1	September 2007	Approved - IGC
V1.1	March 2010	Reviewed by Clinical Quality Manager – submitted to IGG for comment
V2.0	April 2010	Approved by Integrated Governance Committee
V2.1	June 2012	Reviewed by IG Manager
V3.0	23rd February 2015	Review date extension agreed by IGG following approval by EMB
V4.0	17th December 2015	Review date extension Approved by ELB
V5.0	4th August 2016	Approved by ELB

V5.1	11th July 2017	Reviewed – Change of Trust SIRO
V6.0	7th August 2017	Approved Senior Leadership Board

Document Reference	IG Toolkit – Information Governance Framework Requirement Directorate: Clinical Quality Directorate
Recommended at Date	Information Governance Group 25th July 2017
Approved at Date	Executive Leadership Board August 2017
Review date of approved document	August 2019
Equality Impact Assessment	Complete
Linked procedural documents	Information Governance Policy Records Management Policy Information Security Policy Release of Information Policy Internet Use Policy Email Use Policy Freedom of Information Policy
Dissemination requirements	All Trust staff
Checklist completed?	No
Part of Trust's publication scheme	No

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of discriminating, directly or indirectly, against employees, patients, contractors or visitors on the grounds of age, ethnic origin, gender, transgender, sexual orientation, marital status (including civil partnerships), religion & belief, maternity and pregnancy or disability. This policy will apply to all staff regardless of position or status includes volunteers. All East of England Ambulance Service NHS Trust policies can be provided in alternative formats.

Contents

Appendices

1. Introduction

Information governance is a holistic approach to managing clinical, corporate, personal, financial and commercial information by implementing processes, roles, controls and metrics that treat information as a valuable Trust asset. To be a valuable asset, information needs to be relevant, accurate and available to those who have a right to access and use it. The Trust has an established information governance assurance framework in which it operates to ensure all information is handled safely, efficiently and effectively and more importantly fairly and legally. The key principles for the effective use and management of information are collectively represented by HORUS which requires that all information is:

- **H**eld securely and confidentially
- **O**btained fairly and efficiently
- **R**ecorded accurately and reliably
- **U**sed effectively and ethically
- **S**hared appropriately and lawfully

2. Purpose

This Information Governance Strategy has been created to raise awareness of national initiatives, legislation changes and good practice updates so that the Trust can consider what it need to do in the future and how the Trust will get there. The strategic objectives to be achieved over the next four years include those arising from a national perspective as well as those arising from a Trust perspective.This strategy will be used to continue to support the Trust's wider Information Governance Assurance Framework the Information Governance Policy and the Information Governance Work Plan. This strategy will improve the quality of information available to managers, stakeholders, staff and patients. It is hoped that this updated information governance strategy will raise people's awareness of the impending changes to legislation and to NHS guidance.

3. National Perspective Background

3.1 A Paperless NHS: electronic healthcare records

Information technology and information systems used by the NHS have improved greatly in the past decade and this has created many new and useful benefits not only for individual NHS Trusts such as the East of England Ambulance Service NHS Trust but for the patients being served by it. More recently the Government has pledged its commitment to complete the digitisation of the NHS and to deliver a series of important digital milestones on the way to create a paperless NHS by the year 2020. Key milestones include:

- By 2018 to be well on the way to implementing electronic healthcare records
- That these electronic systems are interoperable by 2020
- Patients should be able to access their electronic healthcare record on line
- By 2020 the NHS will be paperless at the point of care.

The introduction of new and improved information technology and the vision to become paperless by the year 2020 arrives when the Trust is facing unprecedented financial constraints at a time of rising demand and increased patient expectation. The arrival of the digital age has often been experienced not as a force for good but rather as an intrusive additional burden in an already pressurised environment. Whilst digital systems for support services within the Trust have had a positive effect, operationally they have been viewed as time consuming and quite often staff have reverted back to paper records when under extreme workload pressures. The Trust has achieved a great deal in the past five years in

digitalizing patient facing systems incorporating ePCR, CAD updates, Hear and Treat systems to name but a few. So what does the Trust need to consider for the future?

In April 2016 Jeremy Hunt announced that there were several miles stones to be achieved towards his paperless NHS target. From 2018 a patient's healthcare record should include information from all their health and care interactions. By the end of 2018 all healthcare professionals should be able access the most up to date lifesaving information across GP surgeries, ambulance services and A&E departments, no matter where a patient is in England. By 2020 this will include social care system as well. A patient care record will be digital, real time and interoperable by 2020. To access the national action plan for implementation go to: Personal Health and Care 2020: Using Data and Technology to Transform Outcomes for Patients and Citizens: A Framework for Action for further information.

The Information Governance groups are asked to consider the implications of this national target and advise on any actions to be taken. Actions can be added to the Information Governance Work Plan. Progress will be monitored by the Information Governance Group on a bi-monthly basis.

3.2 General Data Protection Regulations (GDPR)

New legislation is due to come into force from May 2018. The Data Protection Regulation (GDPR) will introduce a number of changes which the Trust will need to prepare for so that it is compliant and can continue to be registered with the ICO as an Information Controller.

High profile data breaches that left customers' details exposed – such as the TalkTalk breach in November 2015, when hackers broke into systems to steal the personal and bank account data of 157,000 customers – have made individuals acutely aware of the potential risks of sharing their information. They are also more conscious of the extent to which websites, online services and social media are 'invisibly' collecting personal data. The new European General Data Protection Regulation (GDPR) has been developed in response to some of these high profile information breach cases. The GDPR will replace the current 1995 EU Data Protection Directive intending to plug the trust gap, by modernising legislation that safeguards personal data within the EU. It will make protection levels more stringent and will standardise the way regulations are implemented, audited and enforced.

Personal data: Increasing in Scope

Under the new regulations, the definition of 'personal data' is expected to broaden, bringing additional in-scope information into the regulated perimeter. Before adequate governance and security controls can be put in place, the Trust will need to identify what data is being held, where it is stored and how it is being used. Data classification is critical in achieving a greater knowledge of the data that is held, and the first step to a truly data-centric approach to protecting personal information. Patients and Staff will be allowed to request their personal data electronically and indicate the software and format required. This strongly links into the requirement that the Trust will need to be paperless by 2020.

The Information Commissioners Office has published a paper outlining 12 steps which need to be taken now in preparation of the new General Data Protection Regulations (GDPR). It is important to raise awareness of these and other changes and the likely impact.

The Information Governance groups are asked to consider the implications of this change to EU legislation and advise on any actions to be taken. Actions can be added to the Information Governance Work Plan. Progress will be monitored by the Information Governance Group on a bi-monthly basis.

3.3 Information Governance Toolkit (IGT)

The publication of version 14 of the Information Governance Toolkit was published on 31 May 2016 and requires the Trust to achieve level 2 in all requirements if the Trust wishes to continue to expand its business portfolio. The Information Governance Toolkit is an online assessment tool which is managed by the Health and Social Care Information Centre (HSCIC). The HSCIC will be changing its name from 1 July 2016 to NHS Digital.

The IG Toolkit draws together legal requirements and the general condition requirements detailed in the Trust's NHS England Contract. It presents them as a set of specific information governance requirements with which the Trust is expected to comply. The requirement headings include;

- Information Governance
- Management
- Confidentiality and Data Protection Assurance,
- Information Security Assurance,
- Clinical Information Assurance and
- Corporate Information Assurance.

The Trust as a healthcare service provider is subject to a three stage reporting process in which it must submit IG evidence against the 35 IG Toolkit requirements relevant to the Ambulance Service on the following dates:

- 31 July 2016 Baseline Assessment
- 31 October 2016 Performance Update
- 31 March 2017 Final Submission

The completion of the IG Toolkit is mandatory and actions already form part of the Information Governance Work Plan. The Information Governance Group are asked to consider what they feel satisfactory will look like. Level 2 or Level 3 in all requirements and or an improved to the overall percentage score achieved in the Trust's annual submission on 31 March 2016. Progress will be monitored by the Information Governance Group on a bi-monthly basis.

3.4 Data Breaches and Losses

A personal data breach is: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service". A personal data breach may mean that someone other than the data controller gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller's own employee accidentally alters or deletes personal data.

At a national level the Information Commissioners Office has just reported that during the first three months of 2016 there have been 448 incidents registered which constitute a data breach. This is an increase on the same period in 2015 and 2014, when 423 and 445 incidents were reported. The Trust reported 35 level 1 incidents in the first quarter.These incidents include staff mislaying or losing their paper patient care records (PCR's). Others include: Information sent to an incorrect addresses, patient information not faxed to a safe haven fax. Patient information being communicated and over heard by members of the public.

These incidents highlight that there is a gap in way the Trust is handling its personal data. If the Trust is to handle personal data fairly, legally, efficiently, effectively and safely it will need

to improve its risk mitigation processes. TheTrust will continue to report all incidents onto the Datix system and all level 2 incidents will continue to be reported to the HSCIC (NHS Digital). There is a need to reduce the number of data breaches through good risk management techniques.

The Information Governance groups are asked to consider the implications of data breach incidents and advise on any actions to be taken. Actions can be added to the Information Governance Work Plan. Progress will be monitored by the Information Governance Group on a bi-monthly basis.

4. Responsibilities

To implement the Trust's Information Governance Strategy once agreed it will be the responsibility of the Information Governance group to co-ordinate and implement the strategy across the Trust. Other key members of the Staff include:

4.1 Trust Board

The Trust Board has ultimate responsibility for ensuring that the Information Governance Assurance Framework provides a structure in which the Trust operates and handles all information fairly and lawfully.

4.2 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. Details of Serious Untoward Incidents involving data loss or confidentiality breaches must also be detailed in the annual report.

4.3 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is responsible to ensure all information risks are correctly identified, managed and that appropriate assurance mechanisms exist. This is achieved through ownership of the Information Asset Register and ensuring that risk assessment processes are completed and implemented by the Information Asset Owners. Business continuity plans will be reviewed by the SIRO to ensure that all information risks are linked to business continuity plan and are exercised on a regular basis. The SIRO will ensure that the Trust has in place an up to date information mapping diagram which details the Trust's Personal Data processing activities In and Out of the Trust. The Trust's Senior Information Risk Owner is the Executive Director for Strategy and Sustainability.

4.4 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 Trust's Caldicott Guardian is the Medical Director

4.5 Compliance and Standards Lead

The Compliance and Standards Lead is responsible for overseeing the information governance systems and processes within the Trust, raising awareness of information governance issues, and ensuring that good information governance practices are adopted throughout the Trust

4.6 Information Governance Manager

The Information Governance Manager provides day-to-day operational support to the Compliance and Standards Lead. The Information Governance Manager will review the Information Governance Assurance Framework and present the review and updates to the Information Governance Group for approval. The update IGAF will then be submitted to the Executive Leadership Board for approval and sign off. Once signed off the IGAF will be uploaded onto the Trust's public website.

4.7 All Trust Staff

Staff at all levels of the Trust must ensure that they are aware of their obligations with regard to maintaining information security and patient confidentiality, and follow established best practice for information handling at all times.

5. Equality Impact Assessment

An Equality impact Assessment has been undertaken. See Appendix B.

6. Dissemination and Implementation

6.1 Dissemination

This Strategy will be disseminated to staff via the Trust intranet.

6.2 Implementation

Awareness of the Strategy and compliance with its requirements will be promoted via information governance training sessions, such as the induction programme for new Trust staff and annual refresher training for existing staff.

The IG Team will monitor staff compliance with the requirements of the Strategy as part of their on-going work, and take action to rectify any perceived weaknesses in compliance as necessary.

7. Process for Monitoring Compliance and Effectiveness

See Appendix A – Monitoring Table.

The security and integrity of the information processes within EEAST will be monitored for compliance by the Information Governance Group who will escalate any areas of concern to the Performance and Finance Committee.

8. Standards/Key Performance Indicators

The Key Performance Indicator for this Strategy is satisfactory compliance with the requirements of the annual Information Governance Toolkit return.

9. References

- The Common Law Duty of Confidentiality
- Data Protection Act 1998
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- The Human Rights Act 1998 (article 8);
- Computer Misuse Act 1990
- ISO 9000 Information Security Management
- The Children Act 1989
- The Children Act 2004
- Records Management: NHS Code of Practice
- Caldicott Guardian seven principles
- IG Toolkit
- Electronic Communications Act 2000
- A Paperless NHS: Electronic Health Records
- ePCR Contract
- ICO preparing for the General Data Protection Regulations
- Patient Health Care Records and Confidentiality
- ICO Security Breaches
-

10. Associated Documents

Information Governance Assurance Framework
Information Governance Policy
Information Security Policy
Release of Information Policy
Internet Use Policy
Email Use Policy
Freedom of Information Policy

Appendix A – Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Information Governance Toolkit	**Information Governance Team.**	**Progress reports from IG Team.** **Review of interim Toolkit scores.** **Review of independent internal audit reports.**	**Bi-monthly updates at IGG.** **Annual report to Board.**	**Formal written reports.**	**Review by Information Governance Group.** **Formal progress reports will be discussed and required actions and timescales agreed.** **Decisions of the Group will be formally recorded in minutes.**	**Information Governance Manager with support from the IG Team and designated IGG members.**	**Review of processes underpinning the IG Toolkit scores, to improve the Trust's overall IG framework and hence compliance with the requirements of the Toolkit.**
Information Governance Risk Register	**Information Governance Team.** **SIRO.**	**Progress reports from IG Team.** **Monitoring of the Trust Risk Register (4Risk).**	**Bi-monthly updates at IGG.** **Annual report to Board.**	**Summary reports from the 4Risk system.**	**Review by Information Governance Group.** **Ongoing monitoring by the Risk Manager.** **Formal progress reports will be discussed at IGG and required actions and timescales agreed.** **Decisions of the Group will be formally recorded in minutes.**	**Information Governance Manager.** **Other risk leads deemed responsible for the area where the IG risk occurs.**	**Action taken to improve controls and mitigate any IG-related risks, reducing risk score.**
Information Governance Awareness Training	**Information Governance Team.** **Learning and Development.**	**Training completion reports.**	**Monthly reports from LDU.** **Bi-monthly updates at IGG.**	**Formal written reports.**	**Review by Information Governance Group.** **Ongoing monitoring by the Learning and Development Manager.**	**Information Governance Manager.** **Learning and Development Manager.**	**Action taken to ensure that all staff have completed either information governance induction training or annual refresher training.**

	Unit				**Formal progress reports will be discussed at IGG and required actions and timescales agreed.** **Decisions of the Group will be formally recorded in minutes.**		

Appendix B

Equality Impact Assessment: Executive Summary

Executive Summary Page for Equality Impact Assessment:	
Document Reference: Version 4.1	Document Title: IG Strategy
Assessment Date: 22 June 2016	Document Type: Strategy
Responsible Director: Director of Finance.	Lead Manager: Information Governance Manager
Conclusion of Equality Impact Assessment: The Strategy is E&D neutral and has no impact, positive or negative.	
Recommendations for Action Plan: None.	
Risks Identified: None.	
Approved by a member of the executive team:	
YES	**NO**
Name: Kevin Smith	Position: Director of Finance
Signature: - by email -	Date: 22 June 2016
This whole document should be stored with the master document .	