# Information Governance Policy & Framework

## Version 2.2: March 2021

**First Issued:** **October 2016**
**Review date:** **March 2022**

## DOCUMENT CONTROL SHEET

| | |
|---|---|
| **Name of Document:** | Information Governance Policy & Framework |
| **Version:** | 2.2 |
| **File Location / Document Name:** | ECCHO |
| **Date Of This Version:** | March 2021 |
| **Produced By (Designation):** | Business Intelligence Analyst |
| **Reviewed By:** | Risk and Information Governance Team Lead - DPO |
| **Synopsis And Outcomes Of Consultation Undertaken:** | |
| **Synopsis And Outcomes Of Equality and Diversity Impact Assessment:** | |
| **Ratified By (Committee):-** | Information Governance Group |
| **Date Ratified:** | March 2018 |
| **Distribute To:** | All staff |
| **Date Due For Review:** | March 2022 |
| **Enquiries To:** | Information Governance Lead |
| **Approved by Appropriate Group/Committee** | x Date: |
| **Approved by Policy Group** | ☐ Date: |
| **Presented to IGC for information** | ☐ Date: |

## Version Control

| Version Date | Version No. | Author/ Reviewer | Comments |
|---|---|---|---|
| 1 | 25/05/2012 | IG Admin | Draft for Approval |
| 1.1 | 25/01/2014 | IG Admin | Approved by Board |
| 2 | 10/16 | BI Team | Updated for 2016 |
| 2 | March 2018 | Andy Thornton | Periodic review |
| 2.1 | February 2020 | R & IG Team Lead Data Protection Officer | Periodic review – amended job titles & roles & responsibilities |
| 2.2 | March 2021 | R & IG Team Lead Data Protection Officer | Amended year typo DPA 1998 changed to 2018 |

## EQUALITY AND DIVERSITY IMPACT ASSESSMENT

**Impact Assessments must be conducted for:**

- ❑ **All ECCH policies, procedures, protocols and guidelines (clinical and non-clinical)**
- ❑ **Service developments**
- ❑ **Estates and facilities developments**

| | |
|---|---|
| **Name of Policy / Procedure / Service** | **Information Governance Policy and Framework v2** |
| **Manager Leading the Assessment** | |
| **Date of Assessment** | |

## STAGE ONE – INITIAL ASSESSMENT

**Q1. Is this a new or existing policy / procedure / service?**

**☐ New**

**☑ Existing**

**Q2. Who is the policy / procedure / service aimed at?**

**☐ Patients**

**☑ Staff**

**☐ Visitors**

**Q3. Could the policy / procedure / service affect different groups (age, disability, gender, race, ethnic origin, religion or belief, sexual orientation) adversely?**

**☐ Yes**

**☑ No**

**If the answer to this question is NO please sign the form as the assessment is complete, if YES, proceed to Stage Two.**

## Analysis and Decision-Making

**Using all of the information recorded above**, please show below those groups for whom an adverse impact has been identified.

### Adverse Impact Identified?

| | |
|---|---|
| Age | No |
| Disability | No |
| Gender reassignment | No |
| Marriage and civil partnership, | No |
| Pregnancy and maternity | No |
| Race/Ethnic Origin | No |
| Religion/Belief | No |
| Sex | No |
| Sexual Orientation | No |

- Can this adverse impact be justified?
- Can the policy/procedure be changed to remove the adverse impact?

| |
|---|
| If your assessment is likely to have an adverse impact, is there an alternative way of achieving the organisation's aim, objective or outcome |
| What changes, if any, need to be made in order to minimise unjustifiable adverse impact? |

## Contents


1. INTRODUCTION ..... 7
2. SCOPE ..... 7
3. DEFINITIONS ..... 8
4. RESPONSIBILITIES ..... 8
5. POLICY STATEMENT ..... 8
6. TRAINING / SUPPORT ..... 10
7. MONITORING AND REVIEW ..... 10
8. PROCESS FOR MONITORING EFFECTIVE IMPLEMENTATION ..... 11
9. Appendix A: Senior Roles & Responsibilities ..... 11

## 1. INTRODUCTION

1.1 This policy acts as an overall umbrella policy sitting over the other policies relating to each aspect of Information Governance (IG), which provide more detail on the way in which the different initiatives are managed within the organisation. All of the other policies which fall into the various areas of IG; Confidentiality, Data Protection, Records Management etc., are traceable up to the IG Policy.

1.2 Information is a vital asset and plays a key part in clinical governance, corporate governance, and service planning and performance management. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

1.3 The CIC recognises the need for an appropriate balance between openness and confidentiality in the management and use of information, thus ensuring we can account for our actions as a Public Authority by routinely making certain information available to the public whilst equally preserving the confidentiality of personal information about individuals, and commercially sensitive information. The CIC also recognises the need to share identifiable personal information with other health organisations and agencies in a controlled manner consistent with the interests of the individual and, in some circumstances, in the public interest.

1.4 The CIC believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all staff members to ensure and promote the quality of information as this is often used in decision making processes.

## 2. SCOPE

2.1 This policy applies to all East Coast Community Healthcare staff members, whether permanent, temporary or contracted in (either as an individual or through a third party supplier).

2.2 This policy covers Information Governance matters in relation to all of the information assets of East Coast Community Healthcare. There are many types of information asset the CIC is responsible for, including: patient information; databases and data files; contracts and agreements; system documentation; research information; user manuals; training material; operational or support procedures; business continuity plans; fallback arrangements; audit trails; and archived information; specifically:

- software assets: application software, system development tools, and utilities;
- physical assets: computer equipment, communications equipment, removable media, and other equipment;
- services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;
- people, and their qualifications, skills, and experience;
- intangibles, such as reputation and image of the organisation.

## 3. DEFINITIONS

Each supporting CIC Policy will contain a section providing a definition and explanation of terms used within the policy.

## 4. RESPONSIBILITIES

4.1 The East Coast Community Healthcare Risk and Information Governance Team Lead is the individual accountable for Information Governance.

4.2 Line Managers within the CIC are responsible for ensuring that all policies are adhered to, and, where required, are built into local processes, and for ensuring there is on-going compliance with them. Line Managers are also responsible for ensuring that all IG compliance and training requirements are cascaded to staff members.

4.3 All staff members, whether permanent, temporary or contracted-in (either as an individual or through a third-party supplier), are responsible for ensuring that they are aware of the requirements incumbent upon them, and for ensuring that they comply with these policies on a day-to-day basis. All staff contracts and contracts with third parties contain clauses regarding compliance with Information Governance and Confidentiality guidelines. Staff are also provided with a Staff Handbook at their induction which also gives guidance on compliance with Information Governance and Confidentiality guidelines.

4.4 The East Coast Community Healthcare Information Governance Group is responsible for overseeing day-to-day IG issues; developing and maintaining policies, procedures and guidance documents, co-ordinating and raising awareness of IG within the CIC, and for monitoring IG risks. Responsibility for the operation of the IG Group lies with the Risk and Information Governance Team Lead.

## 5. POLICY STATEMENT

5.1 There are 4 key interlinked strands to the IG Policy:

- Openness;
- Legal Compliance;
- Information Security;
- Information Quality Assurance.

5.2 **Openness**

5.2.1 Non-confidential information of the CIC and its services should be made routinely available to the public in accordance with the Freedom of Information Act 2000.

5.2.2 The East Coast Community Healthcare, as a CIC is not a public body and is not, therefore, required to comply with the Freedom of Information Act.

5.2.3 The Duty of Candour is a legal duty on hospital, community and mental health trusts to inform and apologise to patients if there have been mistakes in their care that have led to significant harm. Duty of Candour aims to help patients receive accurate, truthful information from health providers.

5.2.4 ECCH are therefore duty bound, should anything we do cause a patient significant harm or should we make mistakes in care or care delivery, including information governance, to explain the issue in full to the patient. Where a patient is identified as lacking capacity to fully understand the harm or mistake their family/carers will be advised in their best interest.

## 5.3 Legal Compliance

5.3.1 The CIC regards all personal data about individuals and commercially sensitive data as confidential. Confidential data must be processed in accordance with the Human Rights Act 1998, Data Protection Act 2018 and the Common Law Duty of Confidentiality.

5.3.2 The East Coast Community Healthcare Confidentiality Policy is the record which guides staff members in the legal framework that the organisation must comply with when processing confidential information. This policy also contains East Coast Community Healthcare's policy on Data Protection and the confidentiality component of Information Security. Responsibility for the implementation of this policy lies with the Risk and Information Governance Team Lead.

## 5.4 Information Security

5.4.1 Information Security is fundamental to the operation of the CIC due to the confidential data it processes and the reliance on information systems to process and transmit data to the organisation's stakeholders. A risk based approach to information security is adopted by the CIC in line with the requirements laid down by BS ISO/IEC 27001:2005, the British Standard for Information Security Management.

5.4.2 The East Coast Community Healthcare Information Security Policy is the record which guides staff members in the information security policy framework. Responsibility for the implementation of this policy lies with the Head of Information Security.

## 5.5 Information Quality Assurance

5.5.1 All staff members are expected to take ownership of, and seek to improve, the quality of information used within their business area.

5.5.2 Wherever possible, information should be accurate and up-to-date, free from duplication and quality assured at the point of collection.

5.5.3 The East Coast Community Healthcare Records Management Policy is the record, which defines our Records Management (RM) policy and guides staff members in the process of how to manage records during their lifecycle from initial creation, filing, tracking, retention, storage and disposal of records, in a way that is administratively and legally sound. Responsibility for the implementation of this policy lies with the Risk and Information Governance Team Lead.

## 6. TRAINING / SUPPORT

6.1 Staff awareness is critical to the success of IG in the CIC.

6.2 IG training must be provided as part of the staff induction process when staff join the organisation. All new starters are to complete the Introduction to Information Governance eLearning course provided by the IG Training Tool and accessed via ECCH eLearning system (ESR). This requirement will be expected to be undertaken within six weeks of their start date of employment at East Coast Community Healthcare. Managers responsible for managing staff are required to comply with this requirement. If the staff member joining ECCH has an NHS Passport which provides evidence of up to date Information Governance Training this will be accepted in place of the Introduction course.

6.3 IG training must be part of an annual mandatory training programme where staff can update their current knowledge. All staff (including clinical and non-clinical) will complete an annual mandatory Information Governance Refresher module provided by the IG Training Tool and accessed via ECCH eLearning system (ESR).

6.4 Key staff are given additional training to perform their role. All staff in designated roles (e.g. the SIRO, Caldicott Guardian etc.) will be required to review the additional training modules via the Information Governance Training Tool (IGTT) or by another means where professional development can be demonstrated. Each designated role will be required to refresh their IG training modules every three years with the exception of the SIRO who will complete the training annually. All those in specialised roles will be informed by the IG lead of the IG Toolkit requirement to undertake additional IG training. Where modules are not completed within a specific time frame line managers will be contacted to cascade the training requirement.

6.5 IG training should form part of the annual staff appraisal or performance review of staff.

6.6 Training must be provided whenever there is a change in role or responsibilities.

6.7 Further staff training is identified following the Datix investigation relating to an information governance incident.

6.8 IG will form part of the Learning and Development; Statutory and Mandatory Framework.

6.9 A blended learning approach is provided to staff members, using the following:

- NHS IG Training Tool;
- Staff IG Handbook
- IG Communication Materials;
- Staff Awareness Briefings.

## 7. MONITORING AND REVIEW

This Policy will be reviewed annually unless an earlier date is agreed by the Executive Management Board or the IG Group.

## 8. PROCESS FOR MONITORING EFFECTIVE IMPLEMENTATION

8.1 The CIC will use Internal Audit, utilising the centrally provided audit methodology to provide independent assurance of the Information Governance Toolkit return.

8.2 This Policy links to the NHS Digital Data Security and Protection Toolkit performance indicator.

## 9. APPENDICES

### Appendix A: Senior Roles & Responsibilities

| Role | Designated Officer | E-mail |
|---|---|---|
| **Risk and Information Governance Team Lead and Data Protection Officer (DPO)** | **Hannah Lewis**<br>Risk and Information Governance Team Lead and Data Protection Officer | **hannah.lewis15@nhs.net** |
| **Information Security Lead** | **Chris Coleman**<br>Head of ICT | **chrisc@nhs.net** |
| **Caldicott Guardian** | **Paul Benton**<br>Executive Director of Quality | **paul.benton@nhs.net** |
| **Senior Risk Information Owner (SIRO)** | **Simon Bragg**<br>Deputy Chief Executive and Executive Director of Finance & Resources | **simonbragg@nhs.net** |