INFORMATION GOVERNANCE POLICY AND PROCEDURE

Summary

Information Governance stipulates the way in which the NHS should handle information, particularly personal and/or special category information such as patient and staff data. It also enables the Trust to ensure that all confidential information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care to our patients.

Key areas of Information Governance:

- Records Management
- Information Risk
- Information and Cyber Security
- Freedom of Information Act 2000
- Data Protection law such as the General Data Protection Regulation
- Health and Social Care Act 2015
- NHS Codes of Practice.

The aim of this policy is to outline the arrangements required to successfully implement and maintain Information Governance standards.

CONTENTS

1. INTRODUCTION

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services, resources and performance management. It is therefore of paramount importance that the appropriate policies, procedures and management accountability provide a robust governance framework for information management.

The Trust Information Governance Policy has been developed as a result of the work carried out in relation to Controls Assurance Standards, Data Quality, Data Accreditation Programme, Caldicott Review, Data Protection Act 2018, General Data Protection Regulation (GDPR), Information Security and Records Management. It also includes initiatives such as the NHS Confidentiality Code of Practice, Health and Social Care Act

(2015) and Freedom of Information Act 2000. It has also been created in line with the Information Governance Toolkit (IGT), an annual assessment tool managed by the Health and Social Care Information Centre. The IGT has now been replaced with the Data Security and Protection Toolkit which contains 40 assertions replacing the 45 requirements of the previous toolkit.

2. PRINCIPLES OF INFORMATION GOVERNANCE

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust also recognises the need to share information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and in some circumstances, the public interest.

Equally important is the need to ensure high standards of data protection and confidentiality to safeguard personal and commercially sensitive information.

Underpinning this is the integrity need for electronic and paper information to be accurate, relevant, and available to those who need it.

Staff must ensure at all times that high standards of data quality, data protection, integrity, confidentiality and records management are met in compliance with the relevant legislation and NHS guidance. It is the responsibility of all staff to familiarise themselves with this policy and adhere to its principles.

3. MAIN THEMES

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

- Openness
- Legal Compliance
- Information and Cyber Security
- Information Quality Assurance
- National Data Security Standards

Openness

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

The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act.

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

Patients will be able to exercise their right to access information relating to their own health care, their options for treatment and their rights as patients.

The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.

The Trust will have clear procedures and arrangements for handling queries from patients and the public.

Legal Compliance

The Trust regards all identifiable personal information relating to patients as confidential.

The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.

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

The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, General Data Protection Regulation, Human Rights Act and common law confidentiality.

The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

Information and Cyber Security

Information and Cyber Security concerns the comprehensive risk management, protection and resilience of data processing and the digital networks that connect them.

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

The Trust will undertake or commission annual assessments and audits of its information and cyber security arrangements.

The Trust will promote effective confidentiality and security practice to its staff through policies and training.

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

Information Quality Assurance

The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.

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

Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
Wherever possible, information quality should be assured to the point of collection.

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

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

National Data Security Standards

The National Data Guardian (NDG) published the 'National Data Guardian for Health and Care 2017 report: Impact and Influence for patients and service users'. The three key principles that formed the basis of this report are:

1. To encourage sharing of information in the interests of providing care to individuals
2. There should be no surprises to citizens and they should have choice about the use of their data
3. There must be dialogue with the public, helping to increase their knowledge and choices about how data is used to improve health and care.

Following a review of data security, consent and opt outs, the National Data Guardian recommended that the following 10 Data Security Standards are applied in the health and social care system in England:

People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles	
Data Security Standard 1	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.
Data Security Standard 2	All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
Data Security Standard 3	All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Data Security and Protection Toolkit (or provide similar via in-house training programmes).

Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses	
Data Security Standard 4	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
Data Security Standard 6	Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
Data Security Standard 7	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Technology: Ensure technology is secure and up-to-date	
Data Security Standard 8	No unsupported operating systems, software or internet browsers are used within the IT estate.
Data Security Standard 9	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
Data Security Standard 10	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

4. IMPLEMENTATION

Reports will be submitted for consideration by the Board via the Information Governance Committee and the Integrated Governance and Risk Management Committee. The Trust will ensure that the strategy is implemented via the main Information Governance Policy and related policies. All policies, work programmes and action plans will be approved and monitored by the Information Governance Committee and reports will be submitted on a bi-monthly basis. The Information Governance Manager has senior level operational responsibility for this agenda, supporting the Caldicott Guardian in relation to Clinical Governance.

The Trust's Information Governance Committee has responsibility for the formulation of Information Governance policies. This group has senior level representation from all appropriate areas to ensure the Trust steers this agenda in line with current legislation.

The Information Governance Committee will receive reports from designated managers who have responsibility for dealing with all information governance assertions and will approve central returns required by the Data Security and Protection Toolkit to the NHS Digital (NHSD).

The Data Security and Protection Toolkit (DSPT) will be used by the Trust to conduct baseline audit and construct action plans to ensure future compliance with this agenda. The work programmes in the individual areas will be created by adherence to the DSPT standards and to the national standards appropriate to the individual field of activity.

The implementation of policies in this area will be carried out across the Trust by all involved staff and will be led by the Caldicott Guardian and supporting teams.

5. DUTIES / RESPONSIBILITIES

Board of Directors

The Chief Nurse is the Caldicott Guardian for the Trust and an Executive Director of the Board of Directors. The Caldicott Guardian is responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.

The Chief Operating Officer is the Senior Information Risk Owner (SIRO) for the Trust and an Executive Director of the Board of Directors. The SIRO has overall responsibility for the organisation's information risk policy.

The Chief Financial Officer is the Executive lead for IT and Cyber-Security and an Executive Director of the Board of Directors.

The Caldicott Guardian, SIRO and Chief Financial Officer are responsible for reporting any serious Information Governance or data security risks and/or incidents to the Board of Directors.

Data Protection Officer

The Trust Secretary is the Trust's Data Protection Officer (DPO) and assists the organisation in monitoring GDPR compliance, informs and advises on data protection obligations, and provides advice regarding Data Protection Impact Assessments (DPIAs) and is the supervisory authority for data subjects. The DPO will report to the Board of Directors and Council of Governors on relevant matters.

Information Governance Manager

The Trust has an Information Governance Manager to manage the Information Governance agenda and ensuring compliance with the DSPT. This post is line managed by the Director of Performance & Information who has senior operational responsibility for Information Governance. The Information Governance Manager also supports the Caldicott Guardian and SIRO.

Managerial Accountability and Responsibility

All line managers from all operational and corporate services within the Trust are responsible for ensuring that the policy and its supporting strategy, standards, procedures and guidelines are built into local processes and there is ongoing compliance. Breaches of policy will be handled in line with the Trust's Disciplinary Policy.

6. TRAINING REQIUREMENTS

Permanent new staff will receive information governance training and awareness as part of their induction via a face-to-face session and an online e-learning package on the Learning Hub.

Annual mandatory online e-learning Information Governance training is required for all staff (both permanent and temporary). This is available from the Learning Hub training tool and links directly to an individual's training record. Facilitated face-to-face sessions are available on request for staff who do not have access to a computer or require additional training support.

In addition, some roles are required to complete additional annual training, (e.g. the Data Protection Officer; SIRO, Caldicott Guardian, IT Security Specialist) which is available via the NHS Digital e-learning site: https://nhsdigital.e-lfh.org.uk/login

Compliance with the mandatory annual training is monitored by the Information Governance Committee.

7. RISK

The Trust must ensure that it operates within a robust Information Governance framework to reduce the risk of threats such as potential litigation, breach of Data Protection Act and any compromise to patient care. Risk assessments will be carried out in the individual component areas as required by the Data Security and Protection Toolkit. Risk assessments will be undertaken as per the Risk Management Policy with additional Information Governance risk assessments performed if required. Department risk registers will be integrated alongside corporate risk registers.

8. INCIDENT REPORTING

Failure to comply with this policy may result in breaching the GDPR/Data Protection Act (and other legal and regulatory) requirements, resulting in a fine from the Information Commissioner of up to €20m or 4% turnover, whichever is the higher. Where there is a breach of confidentiality or loss/unavailability of data or information asset, this must be reported and managed via the incident reporting process (via the incident reporting system Datix), and in accordance with the "Accident/Incident & Patient Safety Incident Reporting Policy including Serious Incidents Requiring Investigation".

All serious incidents, known as IG SIs, that are rated as Level 2 or above, must be recorded and reported via the NHS Digital Incident Reporting Tool on the NHS Digital DSPT. This will automatically result in a referral to the Information Commissioner's Office and must be reported to the Data Protection Officer as soon as possible. An Initial Management Assessment (IMA) is then carried out, and the severity rating of Level 2 is

confirmed. The Information Governance Manager will then inform the Data Protection Officer, Director of Performance & Information, SIRO, and Caldicott Guardian that a report is to be made.

The Information Governance Manager will update the NHS Digital DSPT reporting tool on a regular basis with regard to the management of the incident, and any response received from the Information Commissioners Office regarding the outcome. Once all actions have been taken to manage the incident, mitigate any risks, and implement the agreed action plan, the incident will be closed.

The Information Governance Committee will receive regular reports of IG incidents; analysis of trends and review copies of Incident Management Reports to ensure the mitigation of the risk, and share learning across the Trust.

9. REVIEW

This policy is reviewed annually by the Information Governance Manager and updated in light of any new guidance received.

10. LINKED DOCUMENTS

Computerised Case Notes Policy and Procedures for (453)

Concerns and Complaints Policy and Procedures (160)

Consent to Examination, Procedure or Treatment Policy (325)

Data Protection Policy (277)

Freedom of Information Policy and Procedures (443)

Information for Patients - Provision and Production Policy (340)

Information Governance Assurance Management Framework (1743)

Management of Medical Records - Policy & Procedures (459)

Records Management Strategy (407)

Risk Management Policy (257)

Transfer of Personal Information Policy (1673)

Appendix 1

Legal and Regulatory Framework

The Trust is bound by the provisions of a number of laws and regulations. The list below is not exhaustive, and other legislation and regulations may also apply.

Laws:

- UK Data Protection Act 2018
- General Data Protection Regulation
- Health & Social Care (Quality & Safety) Act 2015
- Common Law Duty of Confidentiality
- Health & Social Care Act 2012
- National health Service Act 1977 / 2006
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Crime and Disorder Act 1998
- Road Traffic Act 1988
- Electronic Communications Act 2000
- Public Interest Disclosure Act 1998
- Public Records Act 1958, 1967 and 2005

Regulations:

- Caldicott Committee Report 2013
- NHS Confidentiality Code of Practice 2003
- DH Records Management: Code of Practice 2016
- NHS Digital – Data Security and Protection Toolkit – National Data Security Standards
- Care Quality Commission Standards

[End of Document - Do Not Delete]