Thanet Health CIC
Information Governance Policy

Contents

1. Summary

This policy provides an overview of how information will be governed and used in Thanet Health CIC (THCIC); it outlines how the organisation will discharge it duties. This requires a systematic and consistent approach based on controls owned, understood and supported by all those working on its behalf.

THCIC is committed to ensuring that information, in whatever its context, is processed as determined by prevailing law, statute and best practice including the Caldicott 2 report 2013 and its recommendations. Compliance with all organisational policies is a condition of employment and a breach of policy may result in disciplinary action.

2. Scope

This policy covers all aspects of holding, obtaining, recording, using, sharing and disclosing of data/information or records, held in a manual/paper or electronic format, by or on behalf of THCIC.

This includes, but is not limited to; staff employed by the organisation; those engaged in duties for the organisation under a letter of authority, honorary contract or work experience programme; volunteers and any other third party such as contractors, students or visitors.

3. Introduction

THCIC uses information to support the provision and planning of healthcare for patients. Information is also used to support the administration of the NHS and wider Health economy. THCIC depends on the appropriate use Personal Data and management of secondary use of this data.

Information Governance (IG) is a framework to manage information appropriately. To do this we will ensure information is:

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

For personal information it ensures confidentiality and security as well as that processes are in place to ensure appropriate standards of quality and ethical use.

Corporate information and records must also be managed appropriately and, where possible and appropriate, provided to the public to ensure transparency and accountability.

As a provider of services we require good quality information to be created, managed and utilised by our organisation. The organisation is responsible for driving improvements in Information Governance from its services. This ensures an efficient, effective and accountable service. In those instances where we appropriately share or publish information we must ensure that this done in a lawful and appropriate manner.

Information is transferred to other organisations and the suppliers of services to support these functions and disclosed in accordance with statutory, regulatory or organisational requirements. For example, the sharing of clinical data with a patients registered GP is underpinned by a Data Sharing Agreement.

Information forms a key component of the current Government’s Information Revolution for the NHS. This restates the NHS’ intention to ensure effective decision making, inform and empower patients through the provision of accurate, accessible and coherent information.

This organisation must discharge its statutory and organisational responsibilities. All staff, and those working on our behalf, are responsible and contribute towards effective and responsible governance of information in line with the organisation’s aims and objectives.

4. Purpose

The Policy is intended to achieve and maintain the following Information Governance objectives:

Confidentiality

- Ensuring that sensitive information or data is accessible to only authorised individuals, and is not disclosed to unauthorised individuals or the public unless appropriate and lawful;

Integrity

- Safeguarding the accuracy and completeness of information and software, and protecting it from improper modification;

Availability

- Ensuring that information, systems, networks and applications as well as paper records are available when required to departments, groups or users that have a valid reason and authority to access them.

Accountability

- Users will be aware of their responsibilities in relation to their collection, use and processing of data and information.

5. Roles and responsibilities

THCIC has identified the following relevant roles and responsibilities within the organisation.

Role	Responsibilities
THCIC Board	In line with the Guidance for NHS Boards: Information Governance the Board will ensure that its organisation has taken appropriate steps to meet IG standards. In particular it will seek assurance against following questions: 1. "What have we done, as an organisation, to ensure we have implemented adequate policies and procedures and are addressing the responsibilities and key actions required to support effective Information Governance?" 2. "What were the outcomes of our most recent annual Information Governance assessment, and what measures (if any) have been put in place to address identified deficiencies?" 3. "What plans do we have in place to ensure our organisation remains compliant with national standards for Information Governance? 4. "Do we as an organisation have the capacity and capability to guarantee our plans for Information Governance can be implemented?" 5. "Do our information governance arrangements adequately encompass all teams and work areas that we are legally accountable for?" 6. "What plans do we have in place to ensure commitment to the Caldicott 2 recommendations in relation to strengthening our process for managing patients' dissent to use of their information?" 7. "How would we manage FOI requests and Subject Access Requests on disclosure of Information as a result of the Public Information Regulations?"
Accountable Officer	Has overall accountability and responsibility for governance within the organisation. Is provided with assurance, that all risks to the organisation, including those relating to information, are effectively managed and mitigated.
Senior Information Risk Owner (SIRO)	Has overall responsibility for ensuring that effective systems and processes are in place to address the Information Governance agenda. • Foster a culture for protecting and using data. • Ensure information risk requirements are included in the corporate Risk and Issue Management Policy. • Ensure Information Asset Owners (IAOs) undertake risk assessments of their assets. • Be responsible for the Incident Management process ensuring identified information security risks are followed up, incidents managed and lessons learnt. • Provide a focal point for the management, resolution and/or discussion of information risk issues. • Ensure that the THCICs approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff. • Ensure the Board is adequately briefed on information risk issues. • Be accountable for information risk. The SIRO roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance. The role holder will be supported and advised by the IG Team.

Role	Responsibilities
Caldicott Guardian	The role of the Caldicott Guardian is an advisory role acting as the conscience of the organisation for management of patient information and a focal point for patient confidentiality & information sharing issues. Ensures that THCIC completes all requirements in the Caldicott work plan that is relevant to THCIC. These requirements are further linked to the annual IG work plan. The Caldicott Guardian is required to maintain an issues log, which is to be reviewed regularly at Senior management meetings.
IT Security Lead	See Information Security Officer
Information Security Officer	This role will be fulfilled by the THCIC Operational Manager. Provides advice to information owners on potential information risks and controls. Supports in any risk reviews with departments.
Information Asset Owners	All senior staff at Director level are required to act as Information Asset Owners for the information assets within their remit. They will; • Provide assurance to the SIRO that information risk is managed effectively for the information identified as within their remit. • Ensure all Information Assets and flows of data within their remit are identified and logged ensuring each has a legal basis to be processed. • Identify, manage and escalate all information security (for example, dependencies and access control) and information risks as appropriate. The detailed roles and responsibilities are defined in Appendix 1 of the NHS Information Risk Management Guidance

Role	Responsibilities
Information Governance Lead	The Lead Director is responsible for ensuring suitable advice; guidance and support tools and training are available to all staff in the organisation and ensure those who handle data do so appropriately.
All Staff	All those working for THCIC have legal obligations, under the Data Protection Act, common law of confidentiality, and professional obligations, for example the Confidentiality NHS Code of Practice and professional codes of conduct, to manage information appropriately. These are in addition to their contractual obligations which include adherence to policy, and confidentiality clauses in their contract.
Third parties	The same responsibilities apply to those working on behalf of the organisations whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of but not directly employed by the organisation are required to sign a third party agreement outlining their duties and obligations.
Member Practices	This policy should be followed where any member is processing information on behalf of or in relation to the THCIC delivery of its functions. However it is recommended that similar policy standards are in place within each member practice to manage its own data and information.

6. Policy Standards

This policy document sets out the standards that those working for or on behalf of the THCIC are expected to adhere to when handling data or information.

6.1. Accountability and Governance

The THCIC will put in place suitable controls to:

- Assign responsibilities to oversee the delivery of standards set out in this policy
- Report on compliance against Information Governance to the Quality committee within the organisation
- Ensure that all staff have been made aware of their responsibilities, how to comply with them and have available advice and guidance and training programmes to do so
- Ensure the consistency of information governance across the organisation;

- Develop information governance policies and procedures;
- Ensuring compliance with Data Protection, and other information security related legislation;
- Providing support to the team who handle Freedom of Information (FOI) requests;
- Providing support to the Caldicott Guardian and Senior Information Risk Owner (SIRO).

6.2. Managing Information Risk

The THCIC will put in place suitable mechanisms to ensure staff identify and manage information risks in line with existing risk management policy and processes. A failure to effectively implement information could lead to the following risks.

Risk	Example
Reputational Damage	• Making decisions from inaccurate information could undermine any decision and be challenged which could affect the reputation of the individual in question and also the reputation of the company.
Financial Loss	• Loss of information could lead to the following financial penalties based on GDPR: • There will be two levels of fines based on the GDPR. The first is up to €10 million or 2% of the company's global annual turnover of the previous financial year, whichever is higher. The second is up to €20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher. • Inefficient use of information may lead to duplication and wasted time
Failure to comply with legal, regulatory or NHS requirements	• There are a number of lawful requirements to manage information such as the Data Protection Act, Freedom of Information Act, Public Records Act, General Data Protection Regulations (GDPR) and Caldicott Principles which could also lead to reputation or financial loss • Failure to be compliant with NHS Constitution or NHS Care Records Guarantee.

6.3. Openness and Transparency

The THCIC will put in systems and processes to ensure information is made available to the public and individuals as well as make them aware of how to access both this and their own information, e.g.:

- Suitable processes will be put in place to meet requirements of the Freedom of Information Act 2000 and NHS Code of Openness.
- Individuals will be made aware of how their information will be processed using privacy notices, unless legally exempt from the requirement
- Requests for access to personal data will be managed in line with legal requirements and best practice.
- Information, including personal and sensitive data will be shared with other agencies only where there is a legal basis to do so and comply with the Caldicott 2 recommendations.

6.4. Use of information

Information is used, or processed, or created by the organisation for the pursuit of its legitimate business interests and discharge of its statutory functions. All use of information within the organisations and by those working on its behalf must be in accordance with these objectives and obligations.

All information must be used, created and managed in a professional and business-like manner. It must be accessible to the organisation on a long term basis and must be stored in a systematic and consistent manner.

Access to information systems, such as the email, databases, the internet or network, and records of the organisation are provided to staff for business purposes. All access and use must be appropriate and in line with the discharge of their duties.

As staff create information they are doing so on behalf of the organisation, for example when sending emails, and are accountable for the information they create, for its appropriateness and accessibility.

6.5. Personal Confidential Data

Personal Confidential Data (PCD) relates to information about patients, service users and members of staff and can include anything that makes them identifiable. It does not have to include particular demographic information, such as name and address, and can consist of a combination of factors that would make it possible to identify the individual.

Information provided to the NHS is done so on the expectation of confidence and often in a healthcare setting. It is important for staff and working practice to account for this and to ensure that any secondary use of personal data, for non-care purposes, in done in accordance with legal, regulatory and organisational requirements.

The organisation will provide and maintain a privacy notice, or fair processing notice that details what personal data is held and processed, for what purpose it is processed and who it is shared with and what governs that process.

THCIC will provide a clear statement for their area of its responsibility where they process Personal Confidential Data.

A definition of Personal Confidential Data is provided in Appendix C.

6.6. Use of Information to improve performance

The THCIC will actively seek opportunities to improve the performance of the organisation. This includes:

- Use of pseudonymised, anonymised or de-identified patient data to inform better health care decisions for individuals and the community;
- To review processes and functions within the organisation to ensure efficient and effective data processing;
- To engage with partner organisations to support appropriate information sharing which ensures that the patient and public can exercise choice as well as ensuring they are kept informed about proposed uses and sharing of their information.

Any change processes within the organisation are required to be managed and to account for the requirements to ensure appropriate and effective information management. All staff managing change must ensure that they scope potential information governance issues before commencing the change process through completing a Data Protection Impact Assessment.

6.7. Information Security

The THCIC will put in place systems and processes to maintain the security of information where it is required this will include

- Establish and maintain policies for the effective and secure management of its information assets and resources.
- Will undertake or commission annual assessments and audits of its information and IT security arrangements.
- Promote effective confidentiality and security practice to its staff through policies, procedures and training.
- Have in place secure mechanisms for the exchange of information in a variety of forms including but not limited to secure post, email, encrypted storage media etc.
- Encourage safe and secure utilisation of IT services and products to meet efficiency demands whilst still maintaining the suitable availability confidentiality, integrity of the data at all times
- Establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security. Such incidents will be managed in accordance with the Incident reporting guidance https://www.dsptoolkit.nhs.uk/Help/29
- Undertake information risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable information governance controls are in place in relation to the acquisition transfer and storage of data
- Where information risks are assessed these will be considered in line with the international information security standards ISO 27001 and ISO 27005

Further information can be found in the Information Security Policy.

6.8. Information / Records Management

Information is the key resource of the National Health Service (NHS) and the wider health economy; it enables the effective treatment of patients and the management of the NHS system and the services we provide. Information Management requires the management of information from creation, use all the way through to destruction or archival retention.

Appropriate management of information enables an organisation, to reduce costs, improve efficiency and enhance the ability to monitor the performance of our services. Understanding the information we hold and the way our organisation uses it helps us to manage our responsibilities under legislation, such as the Data Protection Act.

The THCIC will ensure that information management principles, controls and standards are in place for each stage of the information's lifecycle. Staff are responsible for maintaining these controls and standards.

In order to support effective provision and to support efficiency, all systems and standard working practice involved in the processing of information must ensure the accuracy and quality of information. The Policy on Information Quality provides more details.

6.9. Information Quality:

The THCIC recognises the importance of quality information to make informed decisions. As such the organisation will ensure processes are in place to maintain:

- **Accessibility** – information can be accessed quickly and efficiently through the use of systematic and constituent filing
- **Accuracy** – information is accurate, with systems that support this work through guidance
- **Completeness** – the relevant information required is identified and working practice ensures it is routinely captured
- **Relevance** – information is kept relevant to the issues rather than for convenience with appropriate management and structure
- **Reliability** - Information must reflect a stable, systematic and consistent approach to collection, management and use.
- **Timeliness** – information is recorded as close to possible to being gathered and can be accessed quickly and efficiently
- **Validity** - Information must be collected, recorded and used to the standard set by relevant requirements or controls.

Further details can be found in the Policy on Information Management.

7. Training

All staff are, as a minimum, mandated to undertake the “Introduction to Information Governance” e-learning module once followed by the “Information Governance Refresher” on an annual basis. Additional training needs analysis will be undertaken and staff should comply with any recommendations identified for their specific job role.

8. Equality and Diversity

As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with expected Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of protected characteristics such as race, social exclusion, gender, disability, age, sexual orientation or religion/belief.

The equality impact assessment has been completed and has identified impact or potential impact as “minimal impact”.

9. Dissemination and Implementation

This policy will be made available to all relevant stakeholders via the THCIC internet site. Additionally this will be made aware via email and included for reference where necessary dependant on need

The policy will be supported by additional related policies and resources to support implementation. This will include the availability of and access to obtain written and verbal advice, guidance and procedures where necessary.

10. Non Conformance with this Policy

Should it not possible to meet the requirements within this policy and associated guidelines this must be brought to the attention of the department’s Information Asset Owner. Any issues will need to be documented as a risk and either:

a. Accepted and reviewed in line with this policy
b. Accepted with a view to implementing and action plan to reduce the risk
c. Not accepted and the practice stop until such time as the risk can be reduced

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures can result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible for.
Failure to maintain these standards can result in criminal proceedings against the individual. These include but are not limited to:

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958

11. Monitoring and Review

Performance against the policy will be monitored against;

- Availability and dissemination of policy and in alternative formats where requested or need identified
- Acceptance and understanding of audience (training, spot checks, surveys)
- Reports of non-conformance i.e. incidents or risks
- Compliance against the Information Governance Toolkit

This policy will be reviewed in accordance with the THCICs governance processes following on an as and when required basis:

- Legislative or case law changes;
- changes or release of good practice or statutory guidance;
- identified deficiencies, risks or following significant incidents reported;
- changes to organisational infrastructure.

Appendices

Appendix A. Evaluation protocol

Monitoring requirements „What in this document do we have to monitor‟	The management of information risks (Information Risk Management) Compliance with the law Compliance with the Information Governance Toolkit Incidents related to the breach of this policy
Monitoring Method	Information Risks will be monitored through the Risk Register and management system. Compliance with law will be monitored through audit, work directed by the Information Governance Toolkit and as directed by the SIRO The Information Governance Toolkit will be monitored by assessment of evidence against the objective of the relevant requirement. In addition, the IGT will be audited by the organisation's internal audit function before the annual submission. Incident reporting and management requirements
Monitoring presented to	THCIC Board and Quality Committee with oversight of Information Governance Senior Information Risk Owner Caldicott Guardian
Frequency of Review	Yearly updates will be provided to the relevant groups, the SIRO and the CG Relevant Information Risks will be added to the Corporate Risk Register and reported in line with Risk Management system Annual (as a minimum) updates to the Board will be provided. The internal audit report on IGT performance will be provided to the Board or delegated sub-committee. Incident Reports will be reviewed on an annual basis and as directed by the seriousness of the incident

Appendix B. Equality and Equity Impact Assessment

This is a checklist to ensure relevant equality and equity aspects of proposals have been addressed either in the main body of the document or in a separate equality & equity impact assessment (EEIA)/ equality analysis. It is not a substitute for an EEIA which is required unless it can be shown that a proposal has no capacity to influence equality. The checklist is to enable the policy lead and the relevant committee to see whether an EEIA is required and to give assurance that the proposals will be legal, fair and equitable.

The word proposal is a generic term for any policy, procedure or strategy that requires assessment.

	Challenge questions	**Yes/ No**	**What positive or negative impact do you assess there may be?**
1.	Does the proposal affect one group more or less favourably than another on the basis of:		
	▪ Race		
	▪ Ethnic origin (including gypsies and travellers, refugees & asylum seekers)		
	▪ Nationality		
	▪ Gender		
	▪ Culture		
	▪ Religion or belief		
	▪ Sexual orientation (including lesbian, gay bisexual and transgender people)		
	▪ Age		
	▪ Disability (including learning disabilities, physical disability, sensory impairment and mental health problems)		
2.	Will the proposal have an impact on lifestyle? (e.g. diet and nutrition, exercise, physical activity, substance use, risk taking behaviour, education and learning)		
3.	Will the proposal have an impact on social environment? (e.g. social status, employment (whether paid or not), social/family support, stress, income)		
4.	Will the proposal have an impact on physical environment? (e.g. living conditions, working conditions, pollution or climate change, accidental injury, public safety, transmission of infectious disease)		
5.	Will the proposal affect access to or experience of services? (e.g. Health Care, Transport, Social Services, Housing Services, Education)		

An answer of „Yes" to any of the above question will require the Policy lead to undertake a full Equality & Equity Impact Assessment (EEIA) and to submit the assessment for review when the policy is being approved.

Appendix C. Definitions

Term	Definition	Source
Data	Data is used to describe „qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation."	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)[1] based on the Cabinet Office definition
Information	Information is the output of some process that summarises interprets or otherwise represents data to convey meaning.	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
Personal Confidential Data or PCD	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review 'personal' includes the Data Protection Act 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.	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)

[1] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf, p. 24