Tower Hamlets GP Care Group (THGPCG) Information Governance Policy

Date Issued	16/07/2020
Date to be reviewed	Periodically or if statutory changes are required
Title	Information Governance Policy
Supersedes	All previous Policies
This policy will impact on	All staff
Financial Implications	No change
Policy Area	Information Governance
Version No	1.0
Issued By	Quality, Safety & Governance Committee
Author & Policy Review	Hamsa Hassan
Contact Details	hamsa.hassan@nhs.net
Effective Date	July 2020
Review Date	May 2021

Document History

	Committees / Groups / Individual	Date
Reviewed by / Policy Review	Hamsa Hassan, Information Governance	July 2020
Accountable Director	Ruth Walters, Director of Quality and Assurance	July 2020
Approved by	Quality, Safety & Governance Committee	July 2020

Table of Contents

1. Introduction

This policy provides guidance for those who work for THGPCG to understand how to look after the information they need to perform their day to day operations, yet protecting information on behalf of patients and service users in line with law and regulations; Data Protection 2018 and GDPR 2016/679. In doing so, through accurate, accessible, and appropriately governed information.

This document refers to information which includes information, data and records. The Cabinet Office defines data as *'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation'* and information as '*output of some process that summarises interprets or otherwise represents data to convey meaning'.* This definition will be adopted throughout this document.

THGPCG uses information to support the management of healthcare services for patients in Tower Hamlets. Information is also used in the administration of the NHS. In addition to these functions are the statutory duties of NHS England and NHS Digital which form the wider governance structure that THGPCG operate within.

The aims of this policy are;

- To maximise the value of organisational assets by ensuring that data is:
    - Held securely and confidentially
    - Obtained fairly and lawfully
    - Recorded accurately and reliably
    - Used effectively and ethically; and
    - Shared and disclosed appropriately and lawfully.
- To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental. THGPCG will ensure:
    - Information will be protected against unauthorised access
    - Confidentiality of information will be assured
    - Integrity of information will be maintained
    - Information will be supported by the highest quality data

- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained and tested
- Information security training will be available to all staff; and
- All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Governance team.

This policy is part of the collection related to information governance which set out the expected standards and controls around the use of information. The policies are:

- Information Governance Policy
- Confidentiality and Data Protection Policy
- Information Security Policy
- Records Management Policy

The concepts and standards within these policies are interconnected. Obligations and intentions are considered across the suite of policies. The policies sit under an overarching Information Governance Framework which sets out roles and responsibilities and information governance related workplans.

2 - Scope

This policy applies to:

- All information and data held and processed by THGPCG which must be managed and held within a controlled environment, including the personal data of patients and staff, as well as organisational information. It applies to information, regardless of format, and includes legacy data held by the organisation.
- All permanent, contract or temporary staff at THGPCG and any third parties who have access to the THGPCG premises, systems or information. Any reference to staff within this document also refers to those working on behalf of the organisation on a temporary, contractual or voluntary basis.
- Information systems, data sets, computer systems, networks, software and information created, held or processed on these systems, together with printed outputs from these systems.
- All means of communicating information, both within and outside THGPCG in both paper and electronic format, including data and voice communications, emails, post, fax, voice and video conferencing.

THGPCG believes that its internal management processes will be improved by the greater availability of information that will grow by the recognition of information governance as a designated corporate function and help lead to desired outcomes.

3 - Purpose

Information governance ensures processes, confidentiality and security controls are in place and sets standards of quality and ethical use of personal data. Organisational records must also be managed appropriately and where possible provided to the public under the appropriate legislation (Freedom of Information Act 2000 and Environmental Information Regulations 2004) to ensure transparency and accountability.

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

THGPCG must manage their statutory and organisational responsibilities. All staff are responsible and contribute towards effective and responsible governance of information in line with the organisation's aims and objectives.

3.1 Roles & Responsibilities

The roles and responsibilities related to this policy are outlined below;

Governance Committee

THGPCG's Governance Committee is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance; coordinating Information Governance in THGPCG and raising awareness of Information Governance.

Senior Information Risk Owner (SIRO)

The SIRO has responsibility for ensuring that effective systems and processes are in place to address the IG agenda.

- Fosters a culture for protecting and using data.
- Ensures information risk requirements appropriately recorded and monitored as part of THGPCG's overall approach to risk management
- Ensure Information Asset Owners (IAOs) undertake risk assessments of their assets.
- Overall responsibility for the Incident Management process, ensuring identified information security risks are followed up, incidents managed and lessons learnt.
- Provides a focal point for the management, resolution and/or discussion of information risk issues.

- Ensures that THGPCG's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Ensures the Governing Body is adequately briefed on information risk issues.
- Is accountable for information risk.

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.

The Caldicott Guardian is supported in this role by the IG Officer and Data Protection Officer.

Data Protection Officer

The role of the Data Protection Officer is to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, and information sharing agreements.

Information Governance Officer

The IG Officer is responsible for ensuring suitable advice, guidance support, tools and training are available to those at THGPCG who handle data, to ensure they do so appropriately. Additionally, completing data protection impact assessments and information sharing agreements. This role will be the main point of contact for staff.

All Staff (including contractors, temporary staff, volunteers)

All staff working for THGPCG, under the Data Protection Act 2018 and 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

This policy should be followed where any member is processing information on behalf of or in relation to THGPCG's delivery of its functions. However, it is recommended that similar policy standards are in place within each member practice regarding the management of its own data and information.

3.2 Objectives

THGPCG Information Governance Group are committed to ensuring that all:

- Information that relates to patients and staff is processed, protected, and disclosed appropriately to provide improved healthcare and decisions for patients.
- Information related to its functions, activities and decisions must be managed to the appropriate standards.

THGPCG's aims for the management of information and associated risk includes:

- Effective and efficient management of information for the care of service users and the management of the care service.
- Actively advance the management of information to improve the provision of services, information and care of patients.
- Engage with partner organisations and where appropriate and lawful share information to support care and the public interest.
- Discharge its obligations to disclose information in response to lawful requests with due regard to its duties of confidence by following clear and systematic processes.
- Ensure that systems and processes are effective to ensure the confidentiality and security of personal and other sensitive information.
- Ensure that all information and data processed, held and managed is of the highest quality in terms of completeness, accuracy, relevance, accessibility and timeliness.
- Ensure that all information and data is held in a consistent and systematic manner that ensures its accessibility, accuracy and integrity throughout its lifecycle.
- To actively provide information in line with the Freedom of Information Act 2000 and other regulatory or organisation requirements.
- Ensure those working on behalf of THGPCG, are informed, trained and active in the appropriate management of information.
- To ensure that change is undertaken in a structured and systematic manner that ensures information governance issues are dealt with in a timely, proportionate, and appropriate way.

4 –Use of Information

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

Access to information systems, such as the email, the internet or network, and records of the organisation are provided to staff for organisational purposes and remain the property of THGPCG. All access to and use of information must be appropriate and in line and reflected with 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.

When any member of staff processes new information or a new way of processing information, then this must be raised with the Information Governance team and a Data Protection Impact Assessment shall be completed.

4.1 Use of Personal Data

Personal data can relate to information about patients, service users and members of staff that describes an identifiable person. It does not have to include demographic information, such as name and address but can consist of a combination of factors that would make it possible to identify the person. Information provided to the NHS, is done so on the expectation of confidentiality and often in a healthcare setting. If personal data is also subject to a duty of confidentiality, for example because it relates to a patient, we refer to this as personal confidential data. It is important for staff and working practice to account for this and to ensure that any secondary use of personal confidential data, for non-care purposes, is done in accordance with legal and organisational requirements.

THGPCG has a fair processing notice published on it's website, which details what personal data is held and processed, for what purpose it is used, who it is shared with, and what governs that process. Each service within the organisation must provide a clear statement for their area of responsibility.

4.2 Use of Information to improve performance

THGPCG will actively seek new ways and opportunities to improve the performance of the NHS across its service base by the better use of information and data. This includes:

- Use of 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 third party organisations to identify appropriate information sharing which ensures that the patient and public can exercise choice and are kept informed.

All change processes would require a review by Operational Management and a Data Protection Impact Assessment (DPIA). All staff managing change must ensure that they identify any potential information governance requirements when scoping the organisation case for any change.

5 – Data Quality

In order to deliver and support effective services, improving efficiency, all systems and standard working practice involved in the processing of information, must ensure the accuracy and quality of information.

Data quality requires:

- **Accessibility** – information can be accessed quickly and efficiently using 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.
- **Timeliness** – information is recorded as close to possible to being gathered and can be accessed quickly and efficiently.

6 - Disclosure and Sharing Information

As a public organisation, THGPCG can only share personal confidential data when it is legally permissible with its counterparts.

This includes:

- The common law duty of confidence, which extends after death.
- Data protection legislation.

Any basis of disclosure and sharing needs to be understood and clearly stated before it is undertaken. This decision must demonstrate that the disclosure or sharing:

- Is reasonable and done in good faith for a clear intention;
- Lawful and relevant to the purpose intended;
- With grounds that are in the public interest.

Data sharing in the NHS is also governed by the Caldicott Principles which supports the legal framework.

Disclosure or sharing of personal confidential data requires one of the following conditions to be met:

- The informed and valid consent of the individual, balanced against any duty of care and consideration of capability to provide that consent;
- Disclosure is in the public interest, which must demonstrate consideration of the balance of public interest against the individual and provision of a confidential service; or
- Disclosure is in accordance with the law.

The Data Protection and Confidentiality policy outlines all the legal bases' *(from DPA 2018 & GDPR 2016/679)* when processing or sharing personal data and special category data.

All routine sharing of information must be supported by a clear statement that can be made available to the public or patients. This fair processing or privacy notice must detail the type of information being shared, who is it is being shared with and to what purpose and benefit. In addition, all routine information sharing must be accompanied by a current data sharing agreement or legally binding agreement that sets out the all relevant issues, undertakings, and processes for the sharing. Further guidance on this can be made via request to the Information Governance team.

6.1 Public rights of disclosure

All staff are reminded that there are several pieces of legislation that require information to be released to the public, the Freedom of Information Act 2000, Environmental Information Regulations 2004), the subject of personal data (Data Protection Legislation), or those with a claim to the estate of the deceased or lawful right (Access to Health Records 1990).

Freedom of Information Act 2000 and Environmental Information Regulations 2004 applies to information in all formats; this includes emails, voice recordings and images.

To meet this responsibility, all staff are responsible for ensuring that the contents of records are:

- **Accessible** – ensuring that they can be found within a systematic and consistent filing structure.
- **Appropriate** and **relevant** – this includes a professional and appropriate tone.
- Have **Integrity** or completeness – so that they can be used in an ongoing basis.
- **Confidential** – appropriately safeguarded to ensure confidentially with a clear statement of who was provided access to the information.
- **Identified** – systems and staff should ensure that personal identifiable, sensitive, confidential and corporate information is clearly stored and marked as such.

Details of THGPCG's policy on active disclosure and compliance with the Freedom of Information Act is outlined in the organisation's Subject Access Request Policy *(under the relevant sections)*, and associated protocols and procedures.

7 - Transferring of information

All transfers of information within and outside THGPCG must be managed, comply with the information security requirements, and follow a clear process. All teams must have a clear statement of their incoming and outgoing flows of personal data and personal confidential data.

This process must identify:

- The appropriate method, and inherent risks, of the transfer.
- The contact point and details to which the information is routinely transferred. All contact points should identify a team and position, rather than an individual to which the information is being transferred.
- How the transfer is confirmed and completed.

In addition, where the transfer of information involves personal or identifiable data:

- The purpose and justification for transferring the information.
- Security standards of the method of transfer.

It is expected that most transfers of information will be routine and follow an identified process.

The transfers of information within THGPCG and between external organisations must be managed in an appropriate manner and by secure methods with any risks identified and managed.

7.1 Safe Havens

In order to support the appropriate transferring of personal confidential data, the organisation will identify appropriate safe haven locations. Safe havens answer the requirements of the Data Protection Legislation and The NHS Code of Practice: Confidentiality and the NHS Care Record Guarantee. Safe havens have arrangements and procedures in place to ensure personal identifiable or sensitive information can be held, received, and communicated securely.

Where safe haven locations are not available to staff, the relevant safe haven procedure for the method of transmission should be applied, safe haven locations and procedures will be posted on the intranet.

THGPCG does not support the use of physical fax machines and has an appropriate electronic solution in place where a fax is required to be sent. Staff must make every effort to encourage those they communicate with to use secure email and/or software with secure and controlled

access to communicate sensitive information. The first method should always be via an encrypted email via Egress from @nhs.net to @nhs.net

8 - Information Security

The purpose of information security is to ensure business continuity in order to minimise the impact of security-related incidents and to ensure the integrity of the information and data processed by THGPCG, as described in the Information Security Policy.

Information security enables information to be processed and shared with appropriate safeguards in place. It ensures the protection of information and assets as well as identifying and acting on threats to security.

Information security is both the technical and physical. It ranges from the security of networks, to the use of appropriate passwords by staff and storage of confidential information in secure environments.

All staff contribute towards the security of information and Information Asset Owners are required to have a clear statement on the information security and risks in place for the assets within their remit.

Information security has three basic components:

- **Confidentiality**: assuring that sensitive information or data is accessible to only authorised individuals and is not disclosed to unauthorised individuals or the public.
- **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 are held responsible for their use of information.

Further information is detailed in the THGPCG's Information Security Policy.

9 – Training

Training will be dictated by staff roles and all staff, and, as a minimum, are required to undertake MS Teams Information Governance Training or Bluestream Information Governance training annually.

10 - Monitoring and Compliance

This framework and the associated controls: policies, protocols and procedures - will be monitored routinely every six months or when a change is required. The information governance team meet regularly (biweekly) outlining IG and IG risks, and additionally in response to any information incident or enforcement action by the Information Commissioner's Office. Information risk management is a key component of wider assurance and control in setting the priorities for the information governance work plan.

Information Asset Owners, assisted by Information Asset Administrators, will be required to routinely review the risks and information flows associated with the information assets utilised to fulfil the business functions and activities within their realm. These updates must then be sent to the IG team when requested for the annual Data Security and Protection Toolkit (DSPT) submissions.

10.1 - Non-Compliance

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures may result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible. Failure to maintain these standards can result in criminal proceedings against the individual.

11 - Review

This policy will be reviewed every six months, or earlier if there are changes to National Guidance or significant changes to the management of risk across the organisation.

12 – Dissemination and Implementation

Upon approval, the policy will be shared with all members of staff through the 'all staff' email, and also updated on THGPCG intranet page. A team and management briefing will be provided to support this dissemination.