Tower Hamlets GP Care Group (THGPCG) CIC Policy Caldecott Principles and Guidelines	
Category	Information Governance
Policy drafted by	Phalguni Trivedi
Policy Approved by Operational Lead and date	Dr Joe Hall, Dr S Shan, Lisa Henschen and Ayesha Lulat Governance Lead
Policy approved by Board Lead and date	Ayesha Lulat, Governance Lead
Date for review	01/08/2015

Introduction

The Caldicott Report was commissioned in December 1997 by the Chief Medical Officer of England owing to increasing concern about the ways in which patient information was used in the NHS in England and Wales and the need to ensure that confidentiality was not undermined.

Such concern was largely due to the development of information technology in the service, and its capacity to disseminate information about patients rapidly and extensively. One of the recommendations of the report stated that all NHS organisations appoint a Caldicott Guardian to ensure patient-identifiable information is kept secure. (Caldicott Guardian are senior members of staff, preferably at Board level).

Applicability

This policy applies to:

- All employees of the GP Care Group.
- Service users, their families and their carers, throughout their relationship with the GP Care Group.
- The implementation of all other Policies of the GP Care Group.

This is not an exhaustive list as the policy applies to anyone that has dealings with the GP Care Group.

Caldicott Guardian

THGPCG Caldicott Guardian is Dr Phillip Bennett Richards

The Caldicott Guardian ensures that high standards of patient and personal information security and confidentiality are implemented. The Caldicott Guardian ensures that confidentiality is a priority and relevant issues are represented at Board level.

Caldicott Principles

There are six Caldicott principles that also tie in with the seven principles of the Data Protection Act 1998.

The Caldicott standard is based on the following six principles:

- **Justify the purpose(s)** - Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
- **Don't use patient-identifiable information unless it is absolutely necessary** - Patient- identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
- **Use the minimum necessary patient-identifiable information** - Where use of patient- identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
- **Access to patient-identifiable information should be on a strict need-to-know basis** - Only those individuals who need access to patient-identifiable information should have access to
  it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
- **Everyone with access to patient-identifiable information should be aware of their responsibilities** - Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
- **Understand and comply with the law –** Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

Associated Policies

This policy should be read in conjunction with the following policies:

- Information Governance Policy
- Information Security & Confidentiality Policy