Tower Hamlets GP Care Group - CIC

EMIS USER APPLICATION and CONFIDENTIALITY AGREEMENT

Applicant Name:	
Applicant Usual Organisation (or State Self Employed):	

This agreement relates to requirements of the Data Protection Act 1998, the Human Rights Act 1998, the 'common law duty of confidentiality' and the Freedom of Information Act (2000).

1. The following terms apply where an organisation or its staff may gain access to, or have provided to it, personal identifiable information (defined within the terms of the Data Protection Act 1998) when working for, or with the Tower Hamlets GP Care Group. It also applies where the contracted third party is privilege to commercially sensitive information, security related information and any intellectual property of the contracting organisation.

2. The access referred to in point 1 above may include:
- Access to or sharing of information held in any electronic format or on paper
- Information that is part of verbal discussions

3. Any information (personal or organisational) will only be used for agreed purposes.

Agreed purposes are: Direct care of patients
Agreed retention period: Information for direct care of patients is retained within the GP Care Group clinical system only. Information extracted for evaluation purposes shall be retained for no more than 5 years.
Agreed destruction method: Data extracted from the GP Care Group clinical system should be returned to the GP Care Group for destruction.

4. Any work involving access to personal identifiable information will be done by formally authorised staff of the organisation (except as provided in paragraph 5 below). The organisation shall keep a record of all such authorisations.

Information containing a unique number (e.g. NHS, NI or organisational) or a combination of items from the following list is personal identifiable data:
Name, Address, Postcode, Date of Birth, Other Dates (i.e. death, diagnosis), Sex, Ethnic Group or Occupation.

5. Where the Care Group sub-contracts any work it is doing this agreement will be an explicit part of that sub-contract.

6. All personal identifiable information will be treated as confidential and will not be disclosed to any other persons outside the requirements of the above agreed purpose(s), without agreement of the 'data controller'. Any organisational information marked as

'commercial' or 'sensitive' or by implication of the subject could prejudice the commercial interests of either party will be treated as confidential.

7. Use an NHSmail account or EMIS workflow to send and receive personally identifiable data.

8. Where the activities performed by the contractor do not require them to process information but they may become party to it by overseeing or overhearing, they will be required to keep such information confidential.

9. Any breach of the terms of this agreement may result in termination of arrangements (including formal contracts) and legal action may be taken.

10. If this agreement is signed on behalf of an organisation rather than an individual, the organisation is responsible for ensuring their staff/sub-contractors adhere to the terms of this agreement.

Please note that to obtain your EMIS user login you need to complete and sign this form and upload it to our online application form click here

I agree to the above terms and conditions (Recipient/Data Processor)

Print Name:	
Signed:	
Date:	

Representative of the Tower Hamlets GP Care Group (Disclosing party)

Print Name:	
Signed:	
Position:	
Date:	

Reminder – 7 Caldicott Principles for Information Sharing (March 2013 Information Governance Review conducted by Dame Fiona Caldicott)

Principle 1 **- 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.

Principle 2 **- Don't use patient-identifiable information unless it is absolutely necessary**
Patient-identifiable data items should not be used unless there is no alternative.

Principle 3 **- Use the minimum necessary patient-identifiable information**
Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

Principle 4 **- 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.

Principle 5 **- Everyone 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.

Principle 6 **- Understand and comply with the law**
Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

The Information Governance Review, April 2013 (known as Caldicott 2), added a 7th Principle:

Principle 7 **- The duty to share information can be as important as the duty to protect patient confidentiality**
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.