Bolton Clinical Commissioning Group

Confidentiality and Data Protection Policy

Policy Number	**IG002**
Target Audience	**CCG/CSU Staff**
Approving Committee	**CCG Executive**
Date Approved	**January 2014**
Last Review Date	**November 2015**
Next Review Date	**November 2017**
Policy Author	**Senior IG Officer (GMSS)**
Version Number	**V3.0**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	August 2013	M Robinson/ D Sankey	Progress to CCG Executive team for approval
1	September 2013	Approved	CCG Exec Team
1.1	January 2014	Andrea Hughes	Amendment to Section 3
	January 2014	IM&T Ops Board	Approved
1.2	November 2015	IG Team	Review document for approval
3.0	December 2015	IM & T Ops	Approved

Analysis of Effect completed	By: M Robinson	Date: August 2013

Contents

1 Introduction and aims

1.1. Bolton Clinical Commissioning Group (henceforth referred to as "the CCG") has a statutory duty to safeguard the confidential information it holds, from whatever source, that is not in the public domain. The principle of this policy is that no individual or company working for or with the CCG shall misuse any information or allow others to do so.

1.2. The CCG holds confidential information relating to service users, staff and the organisation itself. This information should be treated with respect to ensure confidentiality, integrity and protect it from inappropriate disclosure and to make sure that it is not available to persons unauthorised to see it.

1.3. All staff working in the CCG are bound by a common law duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement of the Data Protection Act 1998 and, for health and other professionals, through their own professions' Codes of Conduct.

1.4. The CCG places great emphasis on the need for the strictest confidentiality in respect of personal data. This applies to manual and electronic records and verbal conversations.

1.5. The CCG is committed to the delivery of a first class confidential service. This means ensuring that all personal service user and staff information is processed fairly, lawfully and as transparently as possible so that the public can:

- understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information where necessary;
- gain trust in the way the CCG handles information;
- understand their rights to access information held about them.

2 Scope

This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

3 Accountability and Responsibilities

3.1 The Chief Officer has ultimate responsibility for the implementation of the provisions of this policy. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements

3.2. Responsibilities will be delegated to:

A Caldicott Guardian who will:

- ensure that the CCG satisfies the highest practical standards for handling personal identifiable/confidential information;
- act as the conscience of the CCG;
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information;
- represent and champion Information Governance requirements and issues at Board level;
- ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff;
- oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

A Senior Information Risk owner (SIRO) will:

- be an Executive Director or Senior Management Board Member;
- take overall ownership of the Organisations Information Risk Policy
- act as champion for information risk on the Board and provide advice to the Accounting Officer on the content of the Organisation's Statement of Internal Control in regard to information risk;
- understand the strategic business goals of the CCG and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed;
- work with NWCSU (supplier of IG) to manage the NHS Information Governance risk assessment and management processes within the CCG;
- advise the Board on the effectiveness of information risk management across the CCG;
- receive training as necessary to ensure they remain effective in their role as SIRO.

Information Asset Owners (IAO) will:

- lead and foster a culture that values, protects and uses information for the success of the CCG and benefit of its customers;
- know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset;
- know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy;

- understand and address risks to the asset, and providing assurance to the SIRO.

Information Governance Supplier, Greater Manchester Shared Services (GMSS) will:

- manage the Information Governance Team to deliver Information Governance for the CCG;
- maintain an awareness of information governance issues within the CCG;
- review and update the information governance policy in line with local and national requirements providing template documents to the CCG;
- ensure that line managers are aware of the requirements of the Information Governance policy.

3.3 Line managers will take responsibility for ensuring that the Information Governance Policy is implemented within their staff group or directorate, including any temporary or contract staff.

It is the responsibility of each employee to adhere to the policy.

Staff will receive instruction and direction regarding the policy from a number of sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training course;
- other communication methods, for example, team meetings; and staff Intranet.

All individuals (including any temporary or contract staff) will be required to comply with this policy whilst working within the CCG and thereafter for as long as the information remains confidential information.

All staff (including any temporary or contract staff) are mandated to undertake the “Introduction to Information Governance” e-learning module. Information Governance training is required to be undertaken on an annual basis. The CCG will decide where relevant further training and education will be required of staff. Staff will be informed via the Information Governance Training Needs Analysis.

4 The Duty of Confidence

4.1 All NHS bodies and those carrying out functions on behalf of the NHS have a duty of confidence to service users and a duty to support professional ethical standards of confidentiality.

4.2. Everyone working for the NHS that handles, stores or otherwise comes across information that is capable of identifying individual service users

has a personal duty of confidence to the service user and to his/her employer.

4.3. The duty of confidence is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.

4.4. Service users expect that information given by them to their doctors, nurses and other members of the healthcare team is treated in confidence and not passed to others without their permission. Similar considerations apply to personal information concerning other individuals, such as staff. Particular care must be taken to avoid inadvertent or accidental disclosure. The underlying principle is that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised staff includes those who are not involved in either the clinical care of the service user or the associated administration processes.

4.5. No personal information, given or received in confidence, may be passed to anyone else without the consent of the provider of the information. This is usually the service user but sometimes another person may be the source (e.g. relative or carer).

4.6. No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information.

4.7. Service users are entitled to object to the use of their personal health data for purposes other than their immediate care.

4.8. The duty of confidentiality owed to a deceased service user must be viewed as being consistent with the rights of living individuals

5 What is Personal Information?

5.1 Personal information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

5.2 Personal identifiable information, or personal data, is strictly defined in the Data Protection Act 1998 to which all organisations processing personal information and all staff within those organisations, must adhere.

5.3 Information that identifies individuals personally must be regarded as confidential, and must not be used unless absolutely necessary.

5.4 Confidential information may include personal information such as name, age, address, and personal circumstances, as well as sensitive personal information (as defined by the Data Protection Act 1998 - DPA) regarding race, health, sexuality, etc.

5.5 If an individual is unclear if information should be classified as confidential, they must discuss the issue with their manager and/or IG contacts who will offer advice.

6 Disclosing Information

6.1 The Confidentiality: NHS Code of Practice provides advice on using and disclosing confidential service user information and has models for confidentiality decisions and all staff must adhere to this guidance.

6.2 Personal information may be disclosed on the basis of informed consent where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality.

6.3 Consent of the individual will be required where a disclosure of personal information is not directly concerned with the healthcare / treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional.

6.4 Under common law, personal information may be disclosed without consent for example:

- in order to prevent abuse or serious harm to others
- where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service.

All individuals must:

- exercise all due care and diligence to prevent unauthorised disclosure of confidential information;
- ensure the physical security of all confidential documents , including storage of files on PCs.

6.5 In most circumstances, police should only be given access to personal records with the patients' consent or a court order. Please speak to the Information Governance Team for guidance on the process. Information should only be released to the police after first consulting your line manager and the Caldicott Guardian.

6.6 Any individual has the right to request to see the information an organisation holds about them. This is called a Subject Access request. Any individual making such a request must do so in writing. Staff should contact Complaints and PALS Team if they encounter anyone asking for their personal information.

6.7 Staff should never give information to a person claiming to be the friend, relative or representative of a member of staff/patient/service user. Breaches of personal information can be very damaging to the individual concerned. This may be regarded as gross misconduct under CCG disciplinary rules.

7 Personnel Information

7.1 In keeping with good Human Resources practice, The CCG retains and processes personal data on its employees. In addition, the CCG may from time to time, retain and process "sensitive personal data" as defined by the DPA for example in relation to sickness and occupational health records, performance reviews, equal opportunities monitoring, for the prevention of fraud or other illegal activities.

7.2. The CCG may process such data and such data may be legitimately disclosed to appropriate employees and to CCG professional advisors, in accordance with the principles of the DPA.

7.3. The CCG takes all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that data held on him/ her may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with the Head of Human Resources.

8 Monitoring Review

8.1 This policy will be monitored through staff awareness and supporting evidence to the NHS IG Toolkit

8.2 This policy will be reviewed on an annual basis, and in accordance with the following on an as when basis:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities
- changes to organisational infrastructure.

9 Legislation

The common law Duty of Confidentiality;
Caldicott principles;
Data Protection Act 1998;
Department of Health's "Confidentiality: NHS Code of Practice" including supplementary guidance "Public Interest Disclosures";
The Public Interest Disclosure Act 1998;

10 Other relevant Procedural Documents

- IG012 Secure Transfer of Information Procedure
- IG001 Information Governance Policy
- Freedom of Information Policy
- Information Security Policy
- Disciplinary Policy and Procedure

This list is not exhaustive