Confidentiality Code of Conduct

Version:	4.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Date ratified:	19th September 2017
Name of originator /author (s):	GMSS IG Team
Responsible Committee / individual:	Audit Committee
Date issued:	January 2018
Review date:	December 2019
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Confidentiality Code of Conduct CCG.GOV.021.4.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	GMSS IG Team
This document should be read in conjunction with	Information Governance Policy; Records Management Policy; Information Risk Policy; Freedom of Information Policy; Acceptable Use Policy; Confidentiality Guidelines for staff.
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Published by	NHS Bury Clinical Commissioning Group 21 Silver Street Bury BL9 0EN Main Telephone Number: 0161 762 3100
Copies of this document are available from	CCG Corporate Office CCG Website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
2.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	10th December 2014
3.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	18th November 2015
3.1 = policy review	GMSS IG Team	25th August 2017
4.0 = policy once reviewed	NHS Bury Clinical Commissioning Group Information Governance Operational Group	19th September 2017

Confidentiality Code of Conduct

Table of Contents

1. Introduction

1.1 All organisations have a legal duty to keep all personal information secure and to respect confidentiality when personal information is held in confidence. This requires that all staff are aware of their responsibilities set out within a code of conduct, such as this document, supported by Information Governance policies and procedures.

1.2 Organisations also have a duty to ensure that staff share personal information appropriately when the sharing is for care purposes.

1.3 The Confidentiality Code of Conduct is based on the legal framework and the circumstances under which confidential information can be disclosed such as:

- General Data Protection Regulation (GDPR)
- Data Protection Act 1998
- Confidentiality: NHS Code of Practice
- Records Management: Code of Practice for Health and Social Care 2016
- HSCIC A guide to confidentiality in health and social care: Treating confidential information with respect
- Caldicott Principles and the report "Information – To Share or not to share: The Information Governance Review"
- NHS Care Record Guarantee
- Citizens' rights under the NHS Constitution
- Professional codes of practice

2. Policy Statement

2.1 NHS Bury Clinical Commissioning Group (referred to as the CCG) is committed to enabling those working with information to have an effective understanding of their obligations regarding confidentiality and information security. This document describes those responsibilities and provides guidelines in order to ensure that confidentiality and information security is maintained.

2.2 The Confidentiality Code of Conduct applies to all established and temporary employees, Lay Members, governors, volunteers, students and all individuals who work under a contract for services with the CCG. For the purpose of this policy hereafter these groups will be referred to as `staff`. The Confidentiality Code of Conduct applies whilst these persons are on site and off site as the duty of confidentiality applies even where an individual is not representing the CCG.

3. Key Principles

3.1 The key principle of this Code of Conduct is that no staff shall breach their duty of confidentiality, allow others to do so or attempt to defeat any of CCG's information security systems in order to do so.

CCG has a legal duty to service users and staff (and others who are in contact with the CCG) to:

1. Protect personal confidential information (PCD)
2. Inform how personal confidential data is being/will be/has been used
3. Inform of rights regarding access to personal information

It must be remembered that whilst ordinarily the CCG's policy is to seek consent prior to disclosure of personal information, in certain circumstances the organisation may disclose information without consent.

This Code of Conduct outlines the duty of confidentiality and the CCG's expectations in respect of data processing. Data Processing is anything that the CCG does with data whether this be using, sharing, editing, deleting, transporting or transferring. This code of conduct is designed to ensure that the organisation operates in such a way as to safeguard the confidentiality of personal confidential information.

4. Responsibilities

4.1 Responsibility of the CCG Executive Team

4.1.1 The responsibility for the provision of a Confidentiality Code of Conduct rests initially with the Executive Team.

4.1.2 They will ensure, through the line management structure, that this code of conduct is applied fairly and equitably and that all relevant persons are aware of the standards of conduct required.

4.2 Responsibility of the Information Governance Team & People Services

4.2.1 People Services and the Information Governance Team will oversee the introduction; operation and monitoring of this code of conduct to ensure the fair and consistent application of the policy throughout the CCG.

4.3 Responsibility of the Caldicott Guardian

4.3.1 The Caldicott Guardian will oversee the disclosure of individual personal information with particular attention being paid to extraordinary disclosures (those which are not routine) in accordance with the A Guide to confidentiality in health and social care (HSCIC) and the Caldicott Guardian Manual.

4.4 Responsibility of the Senior Information Risk Owner (SIRO)

4.4.1 The SIRO (who is the Chief Finance Officer), with support from the Information Asset Owners, is responsible for:

- Ensuring that an overall culture exists that values and protects information with the organisation;
- Owns the organisations overall information risk policy and risk assessment process, tests its outcome and ensures that it is used;

- Advising the Chief Officer on the information risk assessment process, test its outcome and ensure that it is used;
- Advising the Chief Officer on the information risk aspect of their Annual Governance Statement;
- Owning the CCG's information incident management framework.

4.5 Responsibility of Managers

4.5.1 Line Managers are responsible for ensuring that staff are aware and understand the Confidentiality Code of Conduct.

4.5.2 Line Managers are responsible for ensuring that staff sign the confidentiality disclaimer (Appendix 2) and that a copy is kept on the employees personal folder and / or accepted electronically via email.

4.6 Responsibility of Employees

4.6.1 Staff are responsible for adhering to the Confidentiality Code of Conduct.

4.6.2 Staff are responsible for signing the confidentiality disclaimer on commencement of employment (see Appendix 1).

4.6.3 Failure to maintain confidentiality in accordance with this code could lead to disciplinary proceedings being brought.

5. What is Personal Confidential Data?

5.1 This is a term introduced by the Caldicott 2 - Information Governance Review and states that PCD is personal information about identified or identifiable individuals, which should be kept private or secret and includes dead as well as living people.

5.2 Examples of identifiable data are:

- Name
- Address
- Postcode
- Date of Birth
- NHS Number

For further information about ensuring personal confidential data remains secure and confidential, please refer to the IG Staff Handbook, ensure you are up to date with Information Governance training and if you do require further help, please contact the Information Governance Team.

6. Data Quality and Record Keeping

6.1 Information must be adequate, relevant and limited to what is necessary (Article 5, 'c' of the GDPR Principles and Principle 3 of the Data Protection Act 1998) and it must be accurate and up to date (Article 5, 'd' of the GDPR Principles and Principle 4 of the

Data Protection Act 1998). All staff in the organisation have a responsibility to ensure personal confidential data is up to date.

6.2 Staff must also ensure that any corporate information is accurate, reliable and up to date (for example, policies and procedures, minutes of meetings, financial information) in order to comply with the above GPDR principles (Article 5), Data Protection Act 1998, the Freedom of Information Act 2000 and the Records Management: NHS Code of Practice for Health and Social Care 2016.

7. Freedom of Information

7.1 The Freedom of Information Act (FoIA), gives the general public right of access to all types of information recorded by public authorities. The CCG has a legal obligation to comply with the Act. Failure to do so is a criminal offence. Compliance with the Act will be monitored by the Information Commissioner's Office (ICO).

7.2 The Act supplements and complements the GDPR and the Data Protection Act 1998, which gives individuals the right to access personal information about them held by the CCG. The Act gives access to all other forms of information which is held by the CCG and it therefore has a more extensive scope than the GDPR and the Data Protection Act 1998. These Acts together will enable the public to access most records held by the CCG.

7.3 You must be aware that potentially any piece of information that has been recorded by staff could be made available to the general public on request.

7.4 You must also ensure that if you are asked to provide information in order to answer a Freedom of Information request this must be responded to within the timescale set with the information provided or with reasons why the information cannot be provided. If you are not the correct person to be dealing with a particular question(s) for a Freedom of Information request, you must inform the Patient Services Team as soon as possible. The CCG has 20 working days to deal with Freedom of Information requests and must ensure timescales are met.

8. The Duty to Share

8.1 The primary concern must be for the health and wellbeing of the individual receiving direct care and the presumption should be in favour of sharing for an individuals' direct care. The CCG adopts the value that staff members are fully supported in their duty to share personal information safely and effectively for direct care purposes and encourages staff to raise concerns with senior staff about barriers to sharing for care.

8.2 The duty to share has also been encompassed within the revised Caldicott Principles. These were revised in September 2013 by the Caldicott 2 Review Panel in their report "Information – To share or not to share: The Information Governance Review." The new Principle 7 states that the duty to share information can be as important as the duty to protect patient confidentiality. This means that health and social care professionals should have the confidence to share information in the best interests of their patients / service users within the framework set out the Caldicott Principles below:

1. Justify the purpose for using the information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need to know basis
5. Everyone must understand their responsibilities
6. Understand and comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality.

9. Protecting and Securing Information

9.1 Confidentiality applies not only to patient records, but also to information about the CCG and about staff. All this information should be handled with care and respect. Breaching confidentiality by computer misuse or any other manner may lead to disciplinary action being taken. It could also call into question any professional registration and could lead to possible legal proceedings.

9.2 Keeping Information Private

9.2.1 The key principles are:

1. Not gossiping – this is an improper use of confidential information, whether it be about CCG, colleagues, patients or service users;
2. Taking care when discussing cases in public places – there are occasions when it is important to discuss cases with colleagues for professional reasons. This can be to gain advice and to share knowledge and experience. Care must be taken to ensure that these discussions cannot be overheard. There would not be a need to reveal the identity of the patient concerned in most cases;
3. Social Engineering – be careful who you are giving information out to whether over the phone, face to face, email. A new term called Social Engineering has been introduced which basically means the art of manipulating people into performing actions or divulging confidential information. Always confirm the identity of the person you are speaking or writing to. Remember the IT Services team will never ask you to disclose your password to them.

9.3 Electronic Security of Information

9.3.1 Personal information must be kept secure. (Article 5, 'e' of the GDPR Principles and Principle 7 of the Data Protection Act 1998). Information about the use of information systems, email and internet can be found in the IT Acceptable Use Policy.

9.3.2 All staff must:

1. Always log out of any computer system or application when work is finished
2. Personally owned memory sticks must not be used.
3. Never leave a computer logged on and unattended, even for the shortest of time – lock your screen if you need to move away from it for a short while (Ctrl, Alt and Delete to lock screen or windows symbol and 'L')
4. All portable equipment (laptops) must be registered with IT Services and must be encrypted

5. Never share / disclose logins / passwords with other staff. If other staff need to access systems, then appropriate access should be organised for them. If staff are found to be sharing passwords this may lead to a disciplinary action being taken in accordance with the CCG's disciplinary policy

The above list is not exhaustive and further information about acceptable use of IT systems and equipment can be found in the IT Acceptable Use Policy. Further information about Information Governance rules can be found in the Information Governance policies and procedures and can be found on the CCG Intranet site.

9.3.3 Some members of staff may be provided with a Smartcard to access data on the national spine (National Care Record Service). The system also maintains a full audit trail of staff accessing records and data. The same principles apply to the use of smartcards as for logins and passwords. All Smartcard holders should adhere to the Registration Authority (RA) Terms and Conditions of Smartcard use as outlined in the RA Policy.

9.3.4 Further information about Information Security and Information Governance can be found via the IG Team. If you are unsure about how to use, share, send personal and / or sensitive information, you must contact the Information Governance Team.

9.4 Manual / paper records

9.4.1 Manual / paper records, containing personal confidential data, must be:

1. Tracked so you know they have been taken and where they have gone;
2. Returned to the filing location as soon as possible;
3. Stored securely within office or clinic, so that the record can be found easily if needed urgently;
4. Stored securely when not in use so that accidental viewing is prevented;
5. Inaccessible to the public and not left, even for the shortest of times, where they could be viewed by an unauthorised person.

9.4.2 Failure to adhere to Information Governance policies may result in monetary penalties being served by the Information Commissioners Office. A monetary penalty notice is a notice requiring a person to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice. The Commissioner may impose a monetary penalty notice if a data controller has seriously contravened the GDPR and the Data Protection Act 1998, if the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the data controller or person must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.

9.5 Physical Security of Assets

9.5.1 All staff must adhere to the IT Acceptable Use Policy regarding security of electronic equipment such as laptops and iPads.

9.5.2 Staff working in an environment where any patient and / or staff records are kept must:

1. Shut / lock doors and cabinets and close windows;
2. Wear ID badges at all times;

3. Query strangers and inform the relevant security staff of suspicious activity.

10. Transportation of Information

10.1 With several methods of communication now available to the CCG, safe haven principles ensure that information is communicated in the most secure way as possible with minimum risk.

10.2 Guidance regarding the secure transportation of personal identifiable and / or sensitive data using the telephone, fax and post can be found in the Secure Transfers of Information Procedure, and guidance can be found on the CCG's website. .

10.3 Please note if you are sending personal and / or sensitive information outside the UK and / or outside the European Economic Area, please inform the Information Governance department to ensure this is transferred safe and securely in compliance with the GDPR. If data is to be transferred overseas, then Chapter 5 (Article 44 – 50) of the GDPR must be observed; 'Transfers of personal data to third countries or international organisations.' Chapter 5 must be applied in order to ensure that the level of protection of natural persons guaranteed by the Regulation is not undermined. In addition Data Protection Act Principle 8 which states that personal information must not be transferred to other countries without adequate protection.

11. Requests for Personal Information (Subject Access Requests)

11.1 Requests for information may come from a variety of sources and it is dependent on the source and type of information requested as to how the request should be handled. Staff should never give out information on patients or staff to persons who do not have a right to access this information.

11.2 Ensure that all requests for personal identifiable and / or sensitive information can be justified on a need to know basis. If a person requests information relating to themselves refer to the CCG's Subject Access Procedure located on the CC's website.

11.3 Access to personal information

11.3.1 Subject Access Requests may be received at the CCG as per the GPDR, Chapter 3, Article 12, which states that personal information must be processed in line with patient's rights. Full details regarding this can be located in the CCG's Subject Access Procedure.

11.4 Access to staff records

11.4.1 Staff may request access to their Human Resource records & personal file. Full details regarding this can be found in the CCG's Subject Access Procedure.

11.5 Requests for information from external bodies

For further information about providing information to external bodies, please refer to the IG Staff Handbook.

12. Retention and Disposal of Information

12.1 Article 5, 'e' of the GDPR Principles and Principle 5 of the Data Protection Act 1998 states that personal information must not be kept longer than necessary. When disposing of confidential waste, staff must use the confidential waste disposal boxes around site and / or a cross cut shredder (not single cut).

12.2 When disposing of IT equipment or removable computer media, IT Services should be contacted. Deleting information from a system does not necessarily mean the data has been removed from the hard drive. Before hard drives are disposed of contact IT Services.

12.3 Both health records and non-health records have assigned minimum retention periods as classified in the Records Management Code of Practice for Health and Social Care 2016.

13. Incident Reporting

13.1 It is imperative that all incidents or near misses relating to the handling of confidential data and / or information security are recorded and reported as soon as possible. This vital feedback allows the CCG to learn from past experience and prevent incidents of a similar nature being repeated.

13.2 Concerns in regard to any potential or actual breaches in confidentiality and / or information security are reportable occurrences and must be reported as soon as possible using incident reporting proforma to report such incidents. Full details can be found in the CCG's Incident Reporting Procedure (located on the website).

14. Training and Improving Knowledge

14.1 It is a compulsory requirement for staff to complete induction training on commencement in post. Information Governance compulsory e-learning training must be completed annually to ensure that staff are fully informed regarding the latest developments within Information Governance. Staff with IG roles must undertake designated IG training modules as detailed in the IG Training Needs Analysis, for further information staff should contact the Information Governance Team. .

14.2 Staff within the CCG are encouraged to be proactive and ask questions if they are unsure about any issues associated with holding, using and sharing personal identifiable and / or sensitive information. Information risk assessments relating to information governance must be produced so these can be investigated and action put in place to mitigate any potential incidents.

15. Social Networking / Media

15.1 Please refer to the IT Acceptable Use Policy regarding use of social networking sites.

16. Auditing

16.1 Confidentiality auditing will focus primarily on control within electronic records management systems but also includes paper record systems and confidentiality processes undertaken by departments, for example safe haven / secure transfer processes. The purpose is to discover whether confidentiality has been breached or put at risk through deliberate misuse of systems as a result of weak, non-existent or poorly applied controls. Assurance that controls are working should be part of the CCG's overall assurance framework.

16.2 Staff emails and internet use are also monitored. Inappropriate access or misuse may result in disciplinary action. For further information, please read the IT Acceptable Use Policy.

16.3 Failure to follow Information Governance policies and utilise information security standards available to staff (such as encryption) to safeguard confidentiality may result in a breach. This contravenes the GDPR, Data Protection Act 1998, the Computer Misuse Act 1990, the Human Rights Act 1998 and the Confidentiality: NHS Code of Conduct.

17. Non - Compliance

17.1 All staff agree to uphold confidentiality on signing their contract of employment and this Confidentiality Code of Conduct. This agreement continues after employment, where relevant, has ceased. Non-compliance with this code may result in disciplinary action being taken in accordance with the CCG's Disciplinary Procedures and in line with the NHS Care Record Guarantee. The guarantee states that the NHS will keep a record of everyone who accesses the electronic information on the NHS Care Records Service and members of the public can ask for a list of everyone who has accessed records.

17.2 Under section of the GDPR (the "Regulation") and the Data Protection Act 1998, the Information Commissioner can serve a monetary penalty on a Data Controller.. Further information can be found on the ICO website (ww.ico.gov.uk).

17.3 The disciplinary procedure and the NHS Care Record Guarantee can be located on the CCG website. Staff should also be aware that they may become personally liable in the civil courts for any breach of confidence that occurs after work for the CCG ends.

18. Monitoring and Review

This policy will be reviewed every 2 years s, and in accordance with the following on an as and when required basis:

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

19. Legislation and Related Documents

A set of procedural document manuals will be available via the CCG staff Intranet.

Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the CCG staff Intranet.

All documents in the CCG Policies and Procedures Register are relevant.

Appendix 1

CONFIDENTIALITY CODE OF CONDUCT DISCLAIMER

Your personal responsibility concerning confidentiality and security of information (relating to patients, staff and the organisation)

Please note that the full Confidentiality Code of Conduct should be read and understood prior to this disclaimer document being signed. If there is anything that is not clear please contact your manager.

The following form is for all staff to sign which includes:
Staff, volunteers and individuals undertaking a contract for services to CCG e.g. Contractors & Agency staff.

During the course of your time within CCG, you may acquire or have access to confidential / personal and / or sensitive information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of CCG. This condition applies during your relationship with the CCG and after the relationship ceases.

Confidential information includes all information relating to CCG. Such information may relate to patient records, business, electronic databases or methods of communication such as use of fax machines, hand-written notes made containing patient information etc. If you are in doubt as to what information may be disclosed, you should check with your manager.

The General Data Protection Regulation and the Data Protection Act 1998 regulates the use of computerised information and paper records of identifiable individuals (patients and staff). The Trust is registered in accordance with this legislation. If you are found to have made an unauthorised disclosure you may face legal and / or disciplinary action.

I understand that I am bound by a duty of confidentiality and agree to adhere to this Confidentiality Code of Conduct and the requirements of the General Data Protection Regulation and the Data Protection Act 1998. .

EMPLOYEE'S NAME:		**MANAGERS NAME**	
TITLE:		**TITLE:**	
DEPARTMENT AND DIVISION:		**DEPARTMENT AND DIVISION:**	
SIGNATURE:		**SIGNATURE:**	
DATE:		**DATE:**	

A COPY OF THIS SIGNED FORM IS TO BE RETAINED IN THE EMPLOYEE'S PERSONAL FOLDER.