Bolton Clinical Commissioning Group

Information Governance Clauses – Clinical and Non Clinical Contracts

Policy Number	**IG014**
Target Audience	**All staff**
Approving Committee	**CCG Exec**
Date Approved	**August 2015**
Last Review Date	**July 2016**
Next Review Date	**August 2018**
Policy Author	**IG Manager**
Version Number	**3**

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	October 2013	Andrea Hughes	Draft
1.1	Aug 2015	IG Team	Formatting changes
2.0	Aug 2015	IM & T Ops	Approved
2.1	**July 2016**	**IM & T Ops**	**Review for Approval**
3.0	**Aug 2016**	**IM & T Ops**	**Approved**

Analysis of Effect completed:	By:	Date:

1. Information Governance Clause

The aim of this Information Governance clause is to ensure that that the supplier / third party / contractor who has access to personal confidential and / or sensitive information, via a service or support arrangement they provide to the CCG, has effective Information Governance requirements in place. This ensures that the confidentiality and security of personal and sensitive information is protected. This in-turn increases public confidence that the NHS and its partners can be trusted with personal confidential data.

The NHS holds the most sensitive and confidential information about individuals and is bound by the Data Protection Act 1998. When sharing data with external parties or is processed by a third party, we must adhere to Principle 7 which states that:

"Appropriate technical and organisational measures shall be taken against unauthorised and or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

Therefore all Data Processors acting on behalf of the CCG or under instruction from the CCG must adhere to the Data Protection Act 1998 and afford the appropriate security to the information it may hold/process where the CCG is the Data Controller. Measures include statements regarding information security, controls for physical security and access control, ensuring Business Continuity is implemented, information governance training for staff and incident reporting procedures. Failure to do so may lead to the CCG seeking damages if a breach/data loss occurs."

Contractors, suppliers and / or third parties are located on-site for a period of time as defined within their contract. They include the following:

- Hardware and software maintenance and support staff
- Cleaning, catering, security guards and any other outsourced support services
- Consultancy and IT contract support staff
- Temporary agency staff

It is important that those who work for contractors, suppliers and / or third parties are aware of Information Governance requirements; what you can and can't do and who you should contact if things go wrong. The CCG also needs to know what security arrangements / controls the third party has in place:

- Do you have adequate security controls, policies and training?
- Are your staff screened prior to commencing employment
- Do you have necessary skills to train your staff regarding confidentiality and data protection or would you like the CCG to assist you with this?

Data protection legislation (Data Protection Act 1998) imposes formal obligations on data controllers (the CCG) that use third party processors to ensure that the processing by the data processor is carried out under a contract, which is made or evidenced in writing, to state that the data processor is to act only on instructions from the data controller.

For the purposes of this document, the term 'contractor' applies to anybody undertaking work for or with the CCG.

All personnel who may come into contact with any Personal Confidential Data (PCD) confidential or sensitive (definitions of each type of data are below) information must follow this agreement. This covers information held manually (for example, on paper) or electronically and also information heard during a visit to any CCG site or access to any

systems containing PCD. It applies to any combination of information, which enables the identification of a patient or a member of staff, either directly or indirectly.
Personal confidential data can be defined as follows:

Personally identifiable data - This relates to information about a person which would enable that person's identity to be established. This might be fairly explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

Sensitive information data - This can be broadly defined as that which if lost or compromised could affect individuals, organisations or the wider community. This is wider than, but includes, personal information defined as sensitive under the Data Protection Act 1998, for example health information are deemed 'sensitive' but the definition may also include financial or security information about an organisation.

Confidential data - A duty of confidence arises when one person discloses information to another (for example patient to a clinician; colleague to colleague; employee to employer; commissioner to contractor) in circumstances where it is reasonable to expect that information will be held in confidence. It -

- is a legal obligation that is derived in case law
- is a requirement established within professional codes of conduct
- must be included within NHS employment contracts as a requirement linked to disciplinary procedures.

The public entrust the NHS with, or allow us to gather, personal and sensitive information relating to the clinical and business activities of the NHS. They do so in confidence and they have a legitimate expectation that all persons who may be exposed to, or process information will respect the confidentially of that information and act appropriately. It is essential, if the legal requirements are to be met and the CCG of the public retained, that the NHS provides, and is seen to provide, a confidential service in all of their clinical and business activities.

2. Rationale

The CCG is under common law duty to ensure that confidential information is protected from inappropriate disclosure. Furthermore, under Principle 1 of the Data Protection Act 1998, personal information must be processed lawfully. This is also emphasised in the Information Governance Toolkit requirements and the NHS Confidentiality Code of Conduct (2003).
The CCG will only be able to comply with these conditions where it has ensured that third parties with whom they have contracts with are subject to, and comply with, patient confidentiality, information security, freedom of information and data protection requirements.

3. Legislation and guidance

The following is a list of legislation and guidance for safeguarding personal identifiable, confidential and sensitive information:

- Information Governance Toolkit (Department of Health / Health and Social Care Information Centre)
- Data Protection Act 1998

- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Computer Misuse Act 1990
- Human Rights Act 1998
- Re-use of Public Sector Information Regulations 2005
- Privacy and Electronic Communications Regulations 2003
- A guide to confidentiality in health and social care (HSCIC) 2013
- Confidentiality: NHS Code of Practice 2003
- Caldicott Principles
- Common Law Duty of Confidentiality
- Records Management: NHS Code of Practice 2006
- NHS Care Records Guarantee, Commitment 9
- Information Security: NHS Code of Practice 2006
- NHS Information Risk Management 2009
- Checklist for the Reporting, Managing and Investigating Information Governance Serious Incident Requiring Investigation (IG SIRI's) 2013

4. Contractor / Suppliers responsibilities

Contractors / Suppliers must ensure that they have read and comply with this agreement and other relevant Information Governance policies and procedures. Contractors must comply with the following:

4.1. Information Governance Toolkit

The supplier / contractor shall work towards achieving standards outlined in the Information Governance Toolkit. This is a useful framework to help organisations comply with Information Governance legislation and the law such as the Data Protection Act 1998. It is expected that organisations attain a minimum level 2 performance against all relevant requirements applicable to it, if they:

a) Have access to personal / sensitive / confidential information via N3 connection
b) Have access to personal / sensitive / confidential information via other means of access – on site, paper copies

Where the supplier / contractor has not achieved the minimum requirement, the Data Controller (the CCG) may, in its sole discretion, agree a plan with the supplier / contractor with enables the CCG to obtain assurance that there are adequate data protection and security arrangements in place. This will be dependant upon the size and turnover of the organisation.

The CCG has the right to audit a contractors / suppliers Information Governance Toolkit assessment as and when required in order to provide assurance.

4.2. Data Protection and Information Security

4.2.1. Notification

The Contractor (where access is required to personal confidential data (PCD) must certify that they are notified with the Information Commissioners Office under the Data Protection Act 1998. To check if you are required to notify, please visit the ICO website (www.ico.gov.uk).

4.2.2. Technical and organisational measures

The Supplier / Contractor must put in place technical and organisational measures against any unauthorised or unlawful processing of personal data, and against any accidental loss or destruction of or damage to such personal data.
The Supplier / Contractor must take reasonable steps to ensure the reliability of staff who will have access to personal data, and ensure that staff are aware of and trained in the policies and procedures relating to Information Governance.

4.2.3. Limitations on disclosure and use of personal confidential data

You must ensure that no personal confidential data (PCD) or sensitive data is transferred, transmitted, disclosed or transported inappropriately to any media, equipment and / or device unless the data is encrypted to the CCG standard and approved.

4.2.4. Security and Data Protection standards

When personal and / or sensitive information is in your custody, it must be kept secure and confidential at all times.

Any personal identifiable data sent from one location to another by or for the contractor shall be carried out utilising safe haven locations and processes at all times. Areas must be risk assessed to ensure personal confidential data is received in a secure area where no unauthorised access may occur.

The CCG shall, where practical, arrange for the equipment or software to be maintained, repaired or tested using dummy data that does not include the disclosure of any personal identifiable data.

If data is to be transferred overseas, then the eighth data protection principle must be observed: Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. (The EEA consists of the EU member states and Iceland, Norway and Liechtenstein). Before a transfer takes place, the Data Controller must be consulted

4.2.5. Restrictions

The Contractor should only act on instructions from the CCG (data controller) regarding the use, transfer and / or storage of information it receives or has access to.
Changes regarding the use of information between the CCG and the contractor should only take place following authorisation by the Information Asset Owner for the system / information asset, or other accountable personnel within the CCG.

5. Freedom of Information

The Freedom of Information Act gives anyone the right to ask any public body for all the information they have on any subject. Unless there's a good reason, the CCG must provide the information within 20 working days.

Most third parties categorise all contracting documentation as confidential and not for disclosure outside of the contracting parties. In light of the Freedom of Information Act this 'confidentiality' may not apply.

As a contractor, you must be aware of the CCG's obligations and its responsibilities under the Freedom of Information Act 2000. This may mean that information which the CCG holds

about your organisation may be subject to disclosure in response to a Freedom of Information request. A document may have been categorised as confidential but the CCG maybe obliged to disclose the document, or parts of it, to an applicant making a request under the Freedom of Information Act 2000.

If you provide any information to the CCG in the expectation that it will be held in confidence then you must make clear in your documentation as to the information to which you consider a duty of confidentiality applies. The use of blanket protective markings such as "commercial in confidence" will no longer be appropriate and a clear indication as to what material is to be considered confidential and why should be provided.

In certain circumstances and in accordance with the code of practice issued under section 45 of the Freedom of Information Act 2000, the CCG may consider it appropriate to ask you for your views as to the release of any information before the CCG makes a decision as to how to respond to a request. In dealing with Freedom of Information requests, the CCG has to comply with strict timetable and it would therefore expect a timely response to any such consultation within the time period stated to you at the time.

The CCG cannot accept that trivial information or information which its very nature cannot be regarded as confidential should be subject to any obligation of confidence.

In certain circumstances where information has not been provided in confidence, the CCG may still wish to consult with you as to the application of any other exemption such as that relating to disclosure may prejudice the commercial interests of any party. However, the decision as to what information will be disclosed will be reserved with the CCG.

5.1. Records Management

A record is anything that contains information, in any media, which has been created or gathered as a result of any aspect of the work carried out. All records need to be managed in a way that allows the information contained within them to be available when they are needed, where they are needed, about whom they are needed by the person who needs them. Contractors must abide by the Records Management: NHS Code of Practice regarding the management of records.

Further information can be sought in the CCG's Corporate Records Management Policy and Corporate Records Management Procedure (available upon request).

6. Incident Reporting

If an Information Governance incident occurs whilst you are working for or on behalf of the CCG, you must report this as soon as possible to your management according to your incident reporting procedures. This must also be reported to the CCG as soon as possible. Please report to the Information Governance Department and / or the Caldicott Guardian. The incident must be formally documented using your organisations incident reporting processes. Any information security or confidentiality breaches made by supplier's employees, agents or sub-contractors must be immediately reported.

The CCG expects an escalation process and action plan in order to resolve problems relating to any incidents / breaches of security and / or confidentiality of personal information by the contractor.

It is imperative that incidents are reported in order:

1. To maintain the security of the CCG's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
2. To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

All CCGs and those who work for or on behalf of the CCG are under a common law duty to ensure that confidential information is protected from inappropriate disclosure. Furthermore, under Principle 1 of the Data Protection Act 1998 personal information must be processed (disclosed) fairly and lawfully. The CCG will only be able to comply with these duties where it has ensured that third parties with whom it contracts are subject to, and comply with, patient confidentiality, information security and data protection requirements.

Definition of an Information Governance (IG) incident - An IG incident is any incident involving the actual or potential loss of personal information that could lead to identify fraud or have an impact on staff or patients. They relate to any breach of security and / or confidentiality.

Examples of such breaches are given below (this list is not intended to be exhaustive):
Breach of security:

- Loss of computer equipment due to crime or an individual's carelessness
- Loss of computer media e.g. memory stick, CD etc due to crime or individual's carelessness
- Trying to access a secure part of the CCG using someone's else's PIN Number, swipe card etc
- Finding the doors and / or windows have been broken and forced entry gained to a secure room / building
- Loss of patient / staff data due to IT software / hardware failure

Breach of confidentiality:

- Finding a computer printout with a header and a person's information on it at a location outside of an CCG premises / buildings
- Looking at confidential patient records on a NHS patient system when you are not directly involved in the care / treatment of that patients in question
- Finding any paper records about a patient / member of staff or business of the CCG in any location outside of the CCG premises / buildings
- Discussing patient or staff personal information with someone else in an open area where the conversation can be heard
- Sending information insecurely using email, post, fax
- A fax being received by an incorrect recipient
- A letter being received by an incorrect recipient

What may at first appear to be of minor importance may on further investigation be found to be serious and vice versa.
The Information Commissioner's Office (ICO) can now issue monetary penalties to a data controller of up to £500,000 for serious breaches of the Data Protection Act 1998 and the Privacy and Electronic Communication Regulations 2003.

7. Monitoring and Review

The CCG reserves the right to audit the contractor or to have those audits carried out by a third party. Monitoring and reviews are designed to ensure that the services in question are being delivered securely and confidentially and that controls are adhered to.

On request, the contractor must supply or allow the CCG to view information governance and security policies, procedures, training records and / or controls to ensure they are acceptable, complete and up to date. If these are not in place, the CCG can audit current practices and / or assist with training and development of such policies / procedures.

Where a contractor has assessed itself meeting the Information Governance assurance requirements to an appropriate level and has recorded its assessment within the Information Governance Toolkit, this must be available for inspection by the CCG to obtain assurances that Information Governance standards are being met. Alternatively, an independent certificate could be provided by the contractor (for example, ISO 27001 certification).

Name of Organisation:	
Name of Individual (Print Name):	
Signature:	
Date:	