Bolton Clinical Commissioning Group

Information Governance Contract Clause

Policy Number	**IG014**
Target Audience	**All staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**28th May 2020**
Last Review Date	**April 2020**
Next Review Date	**28th May 2022**
Policy Author	**IG Team**
Version Number	**V5.1**

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
4.0	June 2018	IG Team	Document IG014 reviewed and completed updated in line with GDPR and NHS Standard Contract GC21 May 2018
4.1	June 2018	IM & T Ops	Approved
5.0	June 2018	CCG Chief Officer	Approved
5.1	April 2020	IG Team	Review for Approval

Analysis of Effect completed:	By:	Date:

Contents Table

Introduction

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

This IG Clause is only required when suppliers / third parties have not used the NHS Standard Contract (which is for clinical services), do not have a contract or their contract does not sufficiently detail IG requirements as required by Data Protection legislation also known as the General Data Protection Regulation (GDPR).

Article 28 of the GDPR states that Data Controllers must only appoint Data Processors who can provide "sufficient guarantees" to meet the requirements of the GDPR.

Whenever a Data Controller uses a Data Processor, there must be a written contract (or other legal act) in place. The contract is important so that both parties understand their responsibilities and liabilities. Contracts also help organisations to comply with the GDPR, and assist Data Controllers in demonstrating to individuals and regulators their compliance as required by the Accountability principle. If a Data Processor uses another organisation (i.e. a sub-processor) to assist in its processing of personal data for a controller, it needs to have a written contract in place with that sub-processor.

Article 28 is clear that Data Processors have obligations such as:

- the data processors liabilities in respect of a breach of GDPR;
- the data processors liability for a breach by one of their sub-contractors.

In addition, Data Controllers and Data Processors must take all measures to ensure the security of the personal data is protected and not compromised, Article 32.

The GDPR sets out what needs to be included in the contract.

To ensure the CCG are adhering to the GDPR the following IG Clause has been taken from the NHS England Standard Contract March 2020 General Conditions (Shorter Form); GC21 Patient Confidentiality, Data Protection, Freedom of Information and Transparency

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:

GC21 Patient Confidentiality, Data Protection, Freedom of Information and Transparency

Information Governance – General Responsibilities

21.1. The Parties must comply with Data Protection Legislation, Data Guidance, the FOIA and the EIR, and must assist each other as necessary to enable each other to comply with these obligations.

21.2. The Provider must complete and publish an annual information governance assessment in accordance with, and comply with the mandatory requirements of, the NHS Data Security and Protection Toolkit, as applicable to the Services and the Provider's organisation type.

21.3. The Provider must:

21.3.1. nominate an Information Governance Lead;

21.3.2. nominate a Caldicott Guardian and Senior Information Risk Owner, each of whom must be a member of the Provider's Governing Body;

21.3.3. where required by Data Protection Legislation, nominate a Data Protection Officer;

21.3.4. ensure that the Co-ordinating Commissioner is kept informed at all times of the identities and contact details of the Information Governance Lead, Data Protection Officer, Caldicott Guardian and the Senior Information Risk Owner; and

21.3.5. ensure that NHS England and NHS Digital are kept informed at all times of the identities and contact details of the Information Governance Lead, Data Protection Officer, Caldicott Guardian and the Senior Information Risk Owner via the NHS Data Security and Protection Toolkit.

21.4. The Provider must adopt and implement the National Data Guardian's Data Security Standards and must comply with further Guidance issued by the Department of Health and Social Care, NHS England and/or NHS Digital pursuant to or in

connection with the Standards. The Provider must be able to demonstrate its compliance with those Standards in accordance with the requirements and timescales set out in such Guidance, including requirements for enabling patient choice.

21.5. The Provider must, at least once in each Contract Year, audit its practices against quality statements regarding data sharing set out in NICE Clinical Guideline 138.

21.6. The Provider must ensure that its NHS Data Security and Protection Toolkit submission is audited in accordance with Information Governance Audit Guidance where applicable. The Provider must inform the Co-ordinating Commissioner of the results of each audit and publish the audit report both within the NHS Data Security and Protection Toolkit and on its website.

21.7. The Provider must report and publish any Data Breach and any Information Governance Breach in accordance with IG Guidance for Serious Incidents. If the Provider is required under Data Protection Legislation to notify the Information Commissioner or a Data Subject of a Personal Data Breach then as soon as reasonably practical and in any event on or before the first such notification is made the Provider must inform the Co-ordinating Commissioner of the Personal Data Breach. This GC21.7 does not require the Provider to provide the Co-ordinating Commissioner with information which identifies any individual affected by the Personal Data Breach where doing so would breach Data Protection Legislation.

Data Protection

21.8. The Provider must have in place a communications strategy and implementation plan to ensure that Service Users are provided with, or have made readily available to them, Privacy Notices, and to disseminate nationally-produced patient information materials. Any failure by the Provider to inform Service Users as required by Data Protection Legislation or Data Guidance about the uses of Personal Data that may take place under this Contract cannot be relied on by the Provider as evidence that such use is unlawful and therefore not contractually required.

21.9. Whether or not a Party or Sub-Contractor is a Data Controller or Data Processor will be determined in accordance with Data Protection Legislation and the ICO Guidance on Data Controllers and Data Processors and any further Data Guidance from a Regulatory or Supervisory Body. The Parties acknowledge that a Party or Sub-Contractor may act as both a Data Controller and a Data Processor. The Parties have indicated in the Particulars whether they consider the Provider to be a Data Processor on behalf of one or more of the Commissioners for the purposes of this Contract.

21.10. The Provider must ensure that all Personal Data processed by or on behalf of the Provider in the course of delivering the Services is processed in accordance with the relevant Parties' obligations under Data Protection Legislation and Data Guidance.

21.11. In relation to Personal Data processed by the Provider in the course of delivering the Services, the Provider must publish, maintain and operate:

21.11.1. policies relating to confidentiality, data protection and information disclosures that comply with the Law, the Caldicott Principles and Good Practice;

21.11.2. policies that describe the personal responsibilities of Staff for handling Personal Data;

21.11.3. a policy that supports the Provider's obligations under the NHS Care Records Guarantee;

21.11.4. agreed protocols to govern the sharing of Personal Data with partner organisations; and

21.11.5. where appropriate, a system and a policy in relation to the recording of any telephone calls or other telehealth consultations in relation to the Services, including the retention and disposal of those recordings,

and apply those policies and protocols conscientiously.

21.12. Where a Commissioner requires information for the purposes of quality management of care processes, the Provider must consider whether the Commissioner's request can be met by providing anonymised or aggregated data which does not contain Personal Data. Where Personal Data must be shared in order to meet the requirements of the Commissioner, the Provider must:

21.12.1. provide such information in pseudonymised form where possible; and in any event

21.12.2. ensure that there is a legal basis for the sharing of Personal Data.

21.13. Notwithstanding GC21.12, the Provider must (unless it can lawfully justify non-disclosure) disclose defined or specified confidential patient information to or at the request of the Co-ordinating Commissioner where support has been provided under the Section 251 Regulations, respecting any individual Service User's objections and complying with other conditions of the relevant approval.

The Provider as a Data Processor

21.14. Where the Provider, in the course of delivering the Services, acts as a Data Processor on behalf of a Commissioner, the provisions of Schedule 6F *(Provider Data Processing Agreement)* will apply.

Responsibilities when engaging Sub-Contractors

21.15. Subject always to GC12 (*Assignment and Sub-Contracting*), if the Provider is to engage any Sub-Contractor to deliver any part of the Services (other than as a Data Processor) and the Sub-Contractor is to access personal or confidential information or interact with Service Users, the Provider must impose on its Sub-Contractor obligations that are no less onerous than the obligations imposed on the Provider by this GC21.

21.16. Without prejudice to GC12 (*Assignment and Sub-Contracting*), if the Provider is to require any Sub-Contractor to act as a Data Processor on its behalf, the Provider must:

21.16.1. require that Sub-Contractor to provide sufficient guarantees in respect of its technical and organisational security measures governing the data processing to be carried out, and take reasonable steps to ensure compliance with those measures;

21.16.2. carry out and record appropriate due diligence before the Sub-Contractor processes any Personal Data in order to demonstrate compliance with Data Protection Legislation; and

21.16.3. as far as practicable include in the terms of the sub-contract terms equivalent to those set out in Schedule 6F *(Provider Data Processor Agreement)* (in any) and in any event ensure that the Sub-Contractor is engaged under the terms of a binding written agreement requiring the Sub-Contractor to:

21.16.3.1. process Personal Data only in accordance with the Provider's instructions as set out in the written agreement, including instructions regarding transfers of Personal Data outside the EU or to an international organisation unless such transfer is required by Law, in which case the Data Processor shall inform the Provider of that requirement before processing takes place, unless this is prohibited by law on the grounds of public interest;

21.16.3.2. ensure that persons authorised to process the Personal Data on behalf of the Sub-Contractor have committed themselves to confidentiality or are under appropriate statutory obligations of confidentiality;

21.16.3.3. comply at all times with those obligations set out at Article 32 of the GDPR and equivalent provisions implemented into Law by DPA 2018;

21.16.3.4. impose obligations as set out in this clause GC21.16.3 on any Sub-processor appointed by the Sub-Contractor;

21.16.3.5. taking into account the nature of the processing, assist the Provider by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Provider's obligation to respond to requests for exercising rights granted to individuals by Data Protection Legislation;

21.16.3.6. assist the Provider in ensuring compliance with the obligations set out at Article 32 to 36 of the GDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to the Sub-Contractor;

21.16.3.7. at the choice of the Provider, delete or return all Personal Data to the Provider after the end of the provision of services relating to processing, and delete existing copies unless the Law requires storage of the Personal Data;

21.16.3.8. create and maintain a record of all categories of data processing activities carried out under the Sub-Contract, containing:

21.16.3.8.1. the name and contact details of the Data Protection Officer (where required by Data Protection Legislation to have one);

21.16.3.8.2. the categories of processing carried out on behalf of the Provider;

21.16.3.8.3. where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards; and

21.16.3.8.4. a general description of the technical and organisation security measures taken to ensure the security and integrity of the Personal Data processed under this Contract;

21.16.3.9. guarantee that it has technical and organisational measures in place that are sufficient to ensure that the processing complies with Data Protection Legislation and ensures that the rights of Data Subject are protected;

21.16.3.10. allow rights of audit and inspection in respect of relevant data handling systems to the Provider or to the Co-ordinating Commissioner or to any person authorised by the Provider or by the Co-ordinating Commissioner to act on its behalf; and

21.16.3.11. impose on its own Sub-Contractors (in the event the Sub-Contractor further sub-contracts any of its obligations under the Sub-Contract) obligations that are substantially equivalent to the obligations imposed on the Sub-Contractor by this GC21.16.3.

21.17. The agreement required by GC21.16 must also set out:

21.17.1. the subject matter of the processing;

21.17.2. the duration of the processing;

21.17.3. the nature and purposes of the processing;

21.17.4. the type of personal data processed;

21.17.5. the categories of data subjects; and

21.17.6. the plan for return and destruction of the data once processing is complete unless the Law requires that the data is preserved.

Freedom of Information and Transparency

21.18. The Provider acknowledges that the Commissioners are subject to the requirements of FOIA and EIR. The Provider must assist and co-operate with each Commissioner to enable it to comply with its disclosure obligations under FOIA and EIR. The Provider agrees:

21.18.1. that this Contract and any other recorded information held by the Provider on a Commissioner's behalf for the purposes of this Contract are subject to the obligations and commitments of the Commissioner under FOIA and EIR;

21.18.2. that the decision on whether any exemption under FOIA or exception under EIR applies to any information is a decision solely for the Commissioner to whom a request for information is addressed;

21.18.3. that where the Provider receives a request for information relating to the Services provided under this Contract and the Provider itself is subject to FOIA or EIR, it will liaise with the relevant Commissioner as to the contents of any response before a response to a request is issued and will promptly (and in any event within 2 Operational Days) provide a copy of the request and any response to the relevant Commissioner;

21.18.4. that where the Provider receives a request for information and the Provider is not itself subject to FOIA or as applicable EIR, it will not respond to that request (unless directed to do so by the relevant Commissioner to whom the request relates) and will promptly (and in any event within 2 Operational Days) transfer the request to the relevant Commissioner;

21.18.5. that any Commissioner, acting in accordance with the codes of practice issued and revised from time to time under both section 45 of FOIA and regulation 16 of EIR, may disclose information concerning the Provider and this Contract either without consulting with the Provider, or following consultation with the Provider and having taken its views into account; and

21.18.6. to assist the Commissioners in responding to a request for information, by processing information or environmental information (as the same are defined in FOIA or EIR) in accordance with a records

management system that complies with all applicable records management recommendations and codes of conduct issued under section 46 of FOIA, and providing copies of all information requested by that Commissioner within 5 Operational Days of that request and without charge.

21.19. The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of FOIA, or for which an exception applies under EIR, the content of this Contract is not Confidential Information.

21.20. Notwithstanding any other term of this Contract, the Provider consents to the publication of this Contract in its entirety (including variations), subject only to the redaction of information that is exempt from disclosure in accordance with the provisions of FOIA or for which an exception applies under EIR.

21.21. In preparing a copy of this Contract for publication under GC21.20 the Commissioners may consult with the Provider to inform decision-making regarding any redactions but the final decision in relation to the redaction of information will be at the Commissioners' absolute discretion.

21.22. The Provider must assist and cooperate with the Commissioners to enable the Commissioners to publish this Contract.

NHS Data Sharing Principles

21.23. The Provider must have regard to the NHS Data Sharing Principles.

Company Name:_____

Signature:_____

Print Name:_____

Designation:_____

Date:_____

Definitions

GDPR

The General Data Protection Regulation forms part of the data protection regime in the UK, together with the Data Protection Act 2018 (DPA 2018). GDPR took effect from 25 May 2018. GDPR applies to Data Controllers and Data Processors who process Personal Data.

Data Controller

A Data Controller determines the purposes and means of processing personal data. A Data Controller must ensure contracts with Data Processors comply with the GDPR.

Data Processor

A Data Processor is responsible for processing personal data on behalf of a Data Controller. Under GDPR Data Processors have specific legal obligations; for example, they are required to maintain records of personal data and processing activities. They will have legal liability if they are responsible for a breach.

Personal Data

This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

Special Categories of Personal Data (previously known as Sensitive Data)

This is personal data consisting of information as to: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. Under GDPR, this now includes biometric data and genetic data.

Personal Confidential Data

This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

Pseudonymised Data or Coded Data

Individual-level information where individuals can be distinguished by using a coded reference, which does not reveal their 'real world' identity. When data has been pseudonymised it still retains a level of detail in the replaced data by use of a key / code or pseudonym that should allow tracking back of the data to its original state.

Anonymised Data

This is data about individuals but with all identifying details removed. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.

Aggregated Data

This is statistical information about multiple individuals that has been combined to show general trends or values without identifying individuals within the data.

Information Governance Lead

Is appointed to act as the overall CCG Information Governance Lead for their organisation.

Caldicott Guardian

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of the patient and service user information and enabling appropriate information sharing.

Data Protection Officer (DPO)

The General Data Protection Regulation (GDPR) May 2018 requires all public authorities to nominate a DPO. This role is a senior role with reporting channels directly to the highest level of management and has the requisite professional qualities and expert knowledge of data protection compliance.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is held by a member of the organisation's Board. They are responsible for identifying and managing the information risks to the organisation.

For a definitive list of Definitions please refer to the NHS Standard Contract 2017/18 and 2018/19 General Conditions (Full Length) (May 2018 edition), 'Definitions and Interpretations' section.

Information Governance Breach

An information governance serious incident requiring investigation, as defined in IG Guidance for Serious Incidents.

Information Commissioner

The independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals ico.org.uk and any other relevant data protection or supervisory authority recognised pursuant to Data Protection Legislation.

National Data Guardian

The body which advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly: https://www.gov.uk/government/organisations/national-data-guardian, and its predecessor body the Independent Information Governance Oversight Panel.

National Data Guardian's Data Security Standards

The standards recommended by the National Data Guardian and approved by the Department of Health and Social Care, as set out in Annex D of Your Data: Better Security, Better Choice, Better Care, available at: https://www.gov.uk/government/consultations/new-data-securitystandards-for-health-and-social-care.

NHS Data Security and Protection Toolkit

An online system (https://www.dsptoolkit.nhs.uk/) which allows NHS Bodies and non-NHS providers of NHS-funded services to assess their compliance with GDPR and with the National Data Guardian's Data Security Standards.

NHS Data Sharing Principles

The document which sets out guiding principles and a framework to help the NHS realise benefits for patients and the public where the NHS shares data with researchers, published by DHSC at https://www.gov.uk/government/publications/creating-the-right-framework-to-realise-the-benefits-of-health-data/creating-the-right-framework-to-realise-the-benefits-for-patients-and-the-nhs-where-data-underpins-innovation.

Legislation and Related Documents

Legal Acts:

- Data Protection Act 2018;
- General Data Protection Regulation;
- Human Rights Act;
- Freedom of Information Act 2000;
- Thefts Act (1968 and 1978);
- Police and Criminal Evidence Act 1984 (PACE);
- Copyright, Designs and Patents Act (1988);
- Computer Misuse Act (1990);
- Trademarks Act (1994);
- Terrorism Act (2000);
- Proceeds of Crime Act (2002);

- Money Laundering Regulations (2007);
- Criminal Justice and Immigration Act (2008);
- Environmental Information Regulations;
- Access to Health Records Act 1990;
- Regulation of Investigatory Powers Act;
- Health and Social Care Act 2006 and ;
- Human Rights Act 1998.

Supporting Documents

- NHS Standard Contract 2017/18 and 2018/19 General Conditions (full length) – May 2018
- Your Data: Better Security, Better Choice, Better Care
- NHS Information Governance: Guidance on Legal and Professional Obligations;
- NHS Code of Confidentiality;
- Information Security Management: NHS Code of Practice April 2007;
- Caldicott Guardian Manual 2017;
- NHS Information Risk Management;
- Records Management Code of Practice for Health and Social Care 2016;
- The Data Security and Protection Toolkit;
- Caldicott 3.