NHS
Bury
Clinical Commissioning Group

Confidentiality Agreement for Third Party Suppliers

Version:	3.0
Ratified by:	NHS Bury CCG Information Governance Steering Group
Date ratified:	July 2021
Name of originator /author (s):	Greater Manchester Shared Services - IT Department; NHS Bury CCG Information Governance Manager
Responsible Committee / individual:	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Date issued:	October 2021
Review date:	July 2023
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Completed Equality Analysis:	Yes

Further information regarding this document

Document name	Confidentiality Third Party Agreement for Suppliers CCG.GOV.028.3.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	Greater Manchester Shared Services - IT Department; NHS Bury CCG Information Governance Manager
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; Safe Transfer of Information Policy (safe haven).
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Development Team; NHS Bury CCG Information Governance Steering Group
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place, Knowsley St Bury, BL9 0SN Main Telephone Number: 0161 762 1500
Copies of this document are available from	The corporate PA office CCG website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
0.1 = draft 1	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	
1.1 = Policy once ratified	NHS Bury Clinical Commissioning	
2.0 = policy once reviewed	IGOG / Quality & Risk Committee	18th November 2015
2.2 = review	NHS Bury CCG, Information Governance Team	October 2021
3.0 = policy once ratified	NHS Bury CCG, Information Governance Steering Group	July 2021

Contents

Table of Contents

1.0 Third Parties Covered by this Agreement

1.1 This document applies to all third parties and their sub-contractors when engaged by NHS Bury Clinical Commissioning Group (hereafter referred to as Bury CCG) in any capacity and for any period. The procuring authority can include directorates, services, teams, or individual managers authorised to engage third party services.

1.2 Third parties will generally be defined within their specific contract, whether working on site or off site. They could include external agencies working under Service level Agreements (SLA's) e.g. SSP, PCSS, SBS, national or local contracts and include the following:

- Hardware and software maintenance and support staff
- Cleaning, catering, security guards and other outsourced support services (contracts should be signed by employing companies and by individual staff)
- Consultancy and IT contract support staff
- Temporary agency staff

1.3 This document includes a number of Appendices which must be completed by all third-party companies or individuals engaged by Bury CCG Appendix A Supplier Certification Form to be completed by all companies/agencies providing staff. Appendix B Individual Contractor Certification Form covers the agreement between individuals and Bury CCG.

1.4 The exceptions to the use of these forms are when contracts have already been agreed with the Department of Health using the contractual templates or the Purchasing and Supply Agency Contracts.

2.0 General Contractor Clause

2.1 The exceptions to the use of these is based on "Introduction to Data Protection in the NHS" (E5127) and (BS ISO/IEC 27001/2)
The Contractor undertakes:

- To treat as confidential all information which may be derived from, or be obtained in the course of the contract, or which may come into the possession of the contractor, or an employee, servant or agent, or sub-contractor of the contractor, as a result, or in connection with the contract; and
- To provide all necessary precautions to ensure that all such information is treated as confidential by the contractor, his employees, servants, agents or sub-contractors; and
- To ensure that he, his employees, servants, agents and sub-contractors are aware of the provisions of the Data Protection Act 2018 and BS ISO/IEC 27001/2, Caldicott Principles and that any personal information obtained from the CCG shall not be disclosed or used in any unlawful manner; and
- To indemnify the NHS organisation (CCG) against any loss arising under the Data Protection Act 2018 caused by any action, authorised or unauthorised, taken by himself, his employees, servants, agents or sub-contractors.

2.2 All employees, agents and/or sub-contractors of the Contractor will be required to agree to and sign a confidentiality statement when they come to any of the CCG sites where they may see, or have access to confidential personal and/or business information. The company confidentiality agreement is shown in Appendix A. The

individual confidentiality agreement is shown in Appendix B.

3.0 Freedom of Information

3.1 The Freedom of Information Act 2000 applies to all the CCG's activities.

3.2 As a partner/customer/agency providing services to the CCG, you should be aware of the CCG's obligations and its responsibilities under the Freedom of Information Act 2000 to provide on request, access to recorded information held by the CCG. One of the consequences is that information which the CCG holds about your organisation may be subject to disclosure in response to a request, unless the CCG decides that one of the various statutory exemptions applies.

3.3 In certain circumstances and in accordance with the code of practice issued under section 45 of the Act, the CCG may consider it appropriate to ask you for your views as to the release of any information before the CCG make its decision as to how to respond to a request. In dealing with requests for the information under the Act, the CCG must comply with a strict timetable, and it would therefore expect a timely response to any such consultation within three working days.

3.4 If you provide any information to the CCG in the expectation that it will be held in confidence, then you must make it 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 given.

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

3.6 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 that will prejudice the commercial interests of any party. However, the decision as to what information will be disclosed will be reserved with the CCG.

4.0 Supplier Code of Practice

Based on example from Introduction to Data Protection in the NHS (E127) and BS27002)

4.1 The following Code of Practice applies where access is obtained to an NHS organisation (CCG) personal data/information, as defined within the Data Protection Act 2018, for the of preventative maintenance, fault diagnosis, hardware or software testing, repair, upgrade or any other related activity.

4.2 The access referred to in paragraph 1 above may include:

a. Access to data/information on the CCGs premises
b. Access to data/information from a remote site
c. Examination, testing and repair of media (e.g. fixed disc assemblies)
d. Examination of software dumps

e. Processing using CCG information

4.3 The Supplier must certify that his organisation is registered appropriately under the Data Protection Act 2018 and legally entitled to undertake the work proposed.

4.4 The Supplier must undertake not to transfer the personal data/information outside of the UK or European Economic Area (EEA) unless such a transfer has been registered, approved by the CCG's Caldicott Guardian and the country to which information is to be transferred has been deemed to have an adequate level of protection for personal information, or is a company which has signed up to other regulatory approved safeguards.

4.5 The Supplier must ensure that they, their employees and any sub contracted staff do not transfer, transmit or transport any Bury CCG sourced or related electronic data / information to or via either their own laptops, computers, servers, USB memory sticks or any other media, portable or otherwise, unless the data is encrypted to the CCG standard. If the media / device(s) do not meet the CCG standard then the data / information must not be transferred, transmitted or transported electronically.

4.6 Anyone who enters areas where staff are working with personally identifiable data needs to be aware that patient data is confidential, not just those who explicitly have access to such data.

4.7 The work shall be done only by authorised employees, servants, or agents of the contractor (except as provided in paragraph 12 below) who are aware of the requirements of the UK UK GDPR and Data Protection Act 2018; in relation to their personal responsibilities under the Act to maintain the security of the CCGs personal data/information.

4.8 While the data/information is in the custody of the contractor it shall be kept in appropriately secure means.

4.9 Any data/information sent from one place to another by or for the contractor shall be carried out be secure means. These places should be within the suppliers own organisation or an approved sub-contractor.

4.10 Data/Information which can identify any patient/employee of the CCG must only be transferred electronically if previously agreed by the CCG and meets internal policies and procedures. This is essential to ensure compliance with strict NHS controls surrounding the electronic transfer of identifiable personal data/information and hence compliance with the Data Protection Act 2018 and BS ISO/IEC 27001/2. This will also apply to any direct-dial access to a computer held database by the supplier or their agent.

4.11 The data/information must not be copied for any other purpose than that agreed by the supplier and the CCG.

4.12 Where personal data/information is recorded in any intelligible form, it shall either be returned to the CCG on completion of the work or disposed of by secure means and a certificate of secure disposal shall be issued to the CCG.

4.13 Where the contractor sub-contracts any work for the purposes in paragraph 1 above, the contractor shall require the sub-contractor to observe the standards set out in

4.11 above.

4.14 The CCG shall, wherever 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 data/information.

4.15 The CCG reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

4.16 The CCG will expect an escalation process for problem resolving relating to any breaches of security and/or confidentiality of personal information by the supplier's employee and/or any agents and/or sub-contractors.

4.17 Contract staff must report any observed or suspected security / confidentiality incident, including weaknesses identified in systems, design or operational procedures that are likely to give rise to an information security incident. This includes the potential disclosure of confidential personal information.

4.18 Any security breaches made by the supplier's employees, agents or sub-contractors will immediately be reported to the Caldicott Guardian, GMSS and the CCG's IG Team and follow the incident reporting procedures within the CCG.

4.19 Demonstration/loan systems with personally identifiable data in any form must have this data removed before equipment is returned.

4.20 If equipment is removed from the premises and it is not immediately possible to securely remove the data then the supplier must secure the data to ensure that no unauthorized access is possible prior to deletion of the data.

4.21 Any major lapse of this agreement will mean that the supplier may be held to be in breach of the contract and therefore subject to potential penalties.

5.0 Third Parties Requiring Access to the Clinical System

5.1 By completing and signing the attached forms the third-party supplier certifies that it understands that:

- Information concerning patients or staff is classified by the CCG as sensitive personal identifiable data (PID) and therefore not to be disclosed to unauthorised persons. This obligation shall continue in perpetuity.
- Disclosures of PID can result in prosecution as an offence under the Data Protection Act 2018 or an action for civil damages under the same act.
- It will not give access to any of the CCGs networks to any external organisation (NHS or otherwise) unless it is legally entitled to undertake the work and has explicit approval given by the CCGs Caldicott Guardian. In such circumstances the Information Commissioner must be appropriately notified that it will be processing personal data.

APPENDIX A

Supplier Certification Form

Name of supplier: ----------

Address of supplier / Prime contractor: ----------

Telephone number: ----------

Email address: ----------

On behalf of the above organisation I certify that:

The organisation is appropriately registered under the UK UK GDPR and Data Protection Act 2018 and is legally entitled to undertake the work agreed in the contract agreed with Bury CCG.

In discharging the contract with Bury CCG the organisation will abide by the requirements set out within this document for the handling of the CCG's personal data / information which is either disclosed or otherwise accessible to my organisation during the period of the contract.

Signed: _____

Name of Individual: _____

Position in organisation: _____

Date: _____

APPENDIX B

Individual Contractor Certification Form

This form is an agreement between individuals contracted to work for Bury CCG, outlining the requirement for the security and confidentiality of data and information relating to patients, staff, and the business of the CCG.

During your period of engagement by Bury CCG you may acquire or have access to personally identifiable or sensitive information, which must not be disclosed to any other person, unless in pursuit of your duties, as detailed in the contract between the Bury CCG and you or your employer.

Confidential information includes all information relating to the business of the CCG and its patients and employees.

The Data protection Act 2018 supplements the UK UK GDPR with respect to the use of all personal information and includes electronic and paper records of identifiable patients and staff. The CCG is registered in accordance with the Data Protection Act and is also bound by the Information Governance standards applicable to all NHS and partner organizations. If you are found to have used or disclosed any information you have seen or heard whilst working within the CCG you or your employer may face legal action.

I understand that I am bound by a duty of confidentiality and I agree to adhere to the conditions in the contract with Bury CCG by which I am engaged and also to my personal responsibilities to comply with the requirements of the Data Protection Act. I also agree to abide by the requirements set out within this document for the handling of the CCGs personal data / information.

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

On behalf of NHS Bury CCG

Managers Name:	
Job Title:	
Signature:	
Date:	

APPENDIX C

Related Policy and Procedures

NHS Bury CCG related policies and guidelines

- Information Governance Framework
- Information Governance Policy
- Records Management Policy
- Confidentiality and Data Protection Policy
- Information Risk Policy
- Information Security Policy
- E-mail Policy
- Encryption Policy
- Acceptable Use Policy