

**Framework Agreement For**

**Data Security and Protection in Confederation Hosted Services and Network Infrastructure**

Document Control

|  |  |  |
| --- | --- | --- |
| Revision History | | |
| Issue | Date | Revision Details |
| Version 1.0 | 21st June 2019 | First Draft |
| Version 1.1 | 29th July 2019 | Final Draft |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
| Author (s) | Simon Boycott – Head of Development and Governance |
| Corporate Lead | Jim Barwick – Chief Executive Officer |
| Document Version | 1.1 |
| Document Status | Draft |
| Date approved by Finance, Performance and Quality Committee |  |
| Review date | August 2020 |

Contents

## Introduction Page 4

## Objectives Page 4

## Purpose, Scope and Governance Page 5

## Parties to the Agreement Page 5

## Framework Agreement and Principles Page 6

## Data Processing Agreement Page 9

## Information Sharing Agreement Page 13

## Smartcard Registration Authority Agreement Page 18

## Signatures Page 20

Appendices

1. Hosted Services Agreement
2. Information Governance Policy and Framework
3. Confidentiality Code of Conduct
4. Data Protection Policy
5. FOI Procedure
6. Information Handling Policy
7. Individual Rights and SAR Procedure
8. Network Security Policy
9. Incident Management and Serious Incidents Policy
10. Records Management Policy
11. Registration Authority Services supporting Information
12. Standard Operating Procedure for Hub Staff Registration
13. Standard Operating Procedure for Extended Access Staff Induction

## Introduction

The emergence of the Leeds GP Confederation as a members organisation and provider of services in the Leeds Health and Social Care sector has brought great opportunities for delivery of primary care services at scale. As a result, there are increased risks relating to the obligations of care providers to protect the information of those who use services and are cared for in primary care services in Leeds.

This framework agreement has been developed to formalise the measures that the Leeds GP Confederation and its members will take to mitigate these risks and to provide assurance to their patients and respective organisations that we will comply with the law and protect their information, and ensure that our joint use of their information and information systems complies with the law.

When in force, this Agreement shall serve as a framework for managing risks to Information Governance and provide assurance to all parties that clinical information systems are being used appropriately, legally, and within the rules that have been agreed.

This framework agreement is made up of 4 parts:

1. An overarching framework agreement which sets out the principles and rules that will be followed when the care delivered to a population stretches across different provider organisation clinical information systems (Clause 5)
2. A Data Processing Agreement to govern the processing of data on individual GP Practice clinical information systems by Confederation employed or Confederation managed/hosted staff (Clause 6)
3. A Data Sharing Agreement to govern access to individual GP Practice DATIX incident reports by Confederation employed or Confederation managed/hosted staff (Clause 7)
4. A Registration Authority Services Agreement to govern the management of smartcard access to GP Practice clinical information systems (Clause 8)

A Hosted Services Agreement is also included to govern the use of the Confederation clinical information system by GP Practice staff and Primary Care Network based staff employed by of managed/hosted by GP Practices (Appendix i).

## Objectives

* 1. The objectives of this Agreement are to:

1. ensure service user rights are respected and to minimise the risk of breaking the law;
2. secure public and partner trust by ensuring that legally required safeguards are in place and complied with;
3. define the policies and processes that GP Practices and the Confederation will employ to protect their patients’ information;
4. set out the way in which clinical information systems will be used to deliver care services at scale;
5. provide a framework for the secure management of information including Patient Confidential Data; and
6. harmonise and support the policies and procedures of each partner organisation regarding the security and confidentiality of data

## Purpose, Scope and Governance

* 1. This document is an Agreement between the Leeds General Practice Confederation, its member practices, and other practices commissioned by NHS Leeds Clinical Commissioning Group.
  2. This Agreement applies to the delivery of any and all services provided by the Leeds GP Confederation on behalf of its members or other parties, services delivered by Primary Care Networks or practices which are supported by the resources and/or infrastructure of the Confederation.

This Agreement is specifically designed to support the delivery of Confederation-hosted services and to support shared or integrated delivery of services where it is necessary for the safe, effective care of the individual service user.

This Agreement is intended to mitigate the risks associated with delivering services at scale and where care pathways extend outside of individual practices or provider organisations.

This Agreement is intended to assure the Confederation, its member practices and other parties, that patient information and information systems are used appropriately, securely and in accordance with the law.

This Agreement is supplemented by the policies, procedures and guidelines of the partner organisations.

This Agreement is owned by the signatory parties.

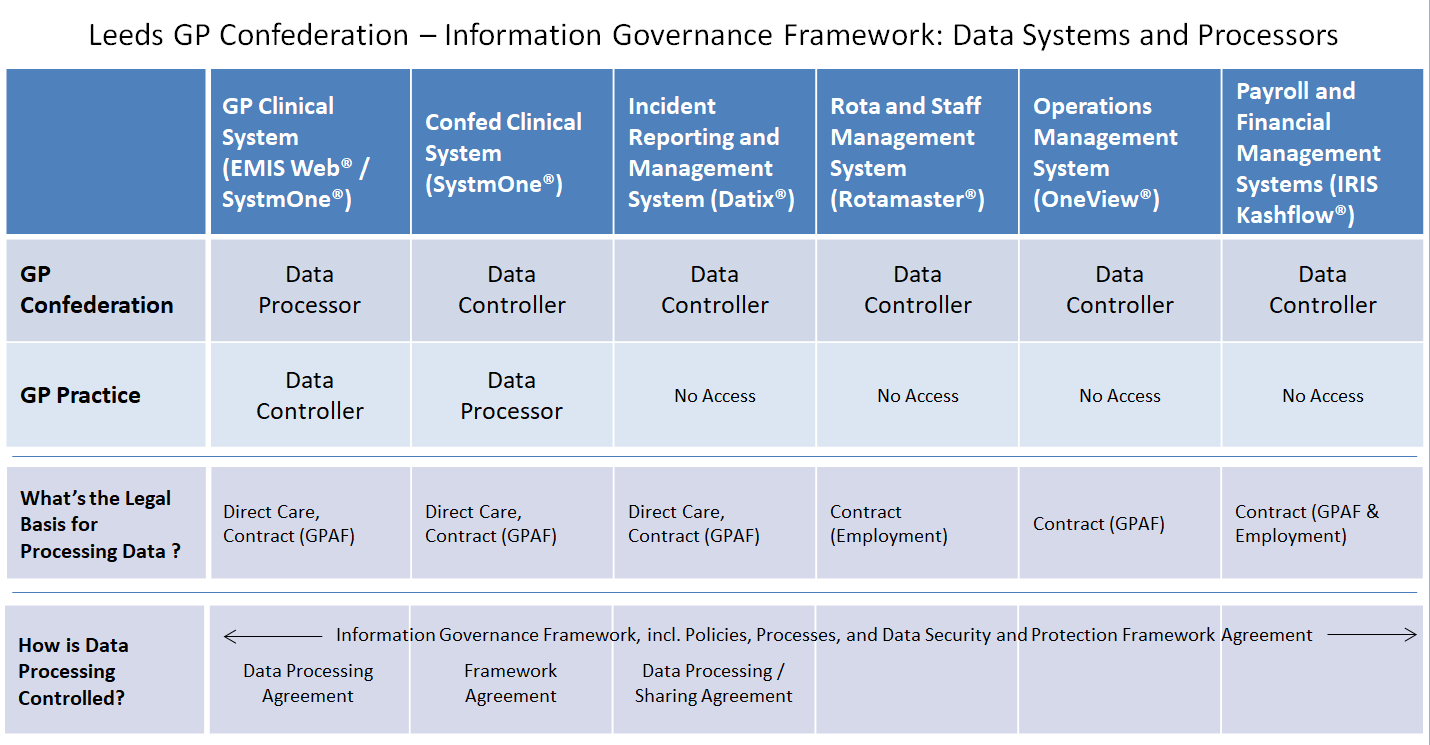
The Quality, Performance and Finance Committee of the Leeds GP Confederation will be responsible for ensuring that this framework agreement is fit for purpose, and for reviewing it every 12 months.

All signatories are responsible for communicating any concerns about the agreement to the Leeds GP Confederation.

## Parties to the Agreement

* 1. The following are parties to this Agreement:
     1. The Leeds General Practice Confederation (‘the Confederation’).
     2. The Primary Care Practice delivering primary medical services under a GMS/PMS/APMS contract with NHS Leeds Clinical Commissioning Group (‘the Practice’).

Figure 1.



## Framework Agreement and Principles

* 1. In the furtherance of activities within the scope of this agreement, the Confederation agrees to the following:
     1. The Confederation will comply with the law and relevant national guidance in all aspects of Data Protection including but not limited to:
        1. General Data Protection Regulation 2016
        2. Data Protection Act 2018
        3. Human Rights Act 1998
        4. Privacy and Electronic Communications Regulations 2003
        5. Health and Social Care (National Data Guardian) Act 2018
     2. The Confederation will comply with Information Governance Framework and policies and will publish these to its members and the public
     3. The Confederation will maintain a suite of policies and procedures to ensure Information Governance of a high standard including;
        1. Information Governance Policy and Framework
        2. Confidentiality Code of Practice
        3. Data Protection Policy
        4. Freedom of Information Procedure
        5. Individual Rights and Subject Access Request Procedure
        6. Information Handling Policy
        7. Network Security Policy
        8. Records Management Policy
     4. The Confederation will ensure that all staff employed by the Confederation who access GP Clinical Information Systems and Confederation systems are appropriately trained, and managed in line with Confederation policies.
     5. The Confederation will ensure that staff comply with the law and Confederation policies when accessing GP Clinical Information Systems.
     6. The Confederation will report any incidents, complaints or concerns from patients involving the use of GP Clinical Information Systems to the GP Practice concerned in a timely manner and work with GP Practices to investigate and resolve them.
     7. The Confederation will ensure that it meets the minimum standards for Information Governance as set out in the DSP Toolkit.
     8. The Confederation will maintain registration with the Information Commissioner’s Office.
     9. The Confederation will audit access to the Confederation Clinical Information System quarterly and take any remedial action needed arising from the audit.
     10. The Confederation will require that all GP Practice-based staff who have access to the Confederation Clinical Information System comply with Confederation policies relating to its use.
     11. The Confederation will ensure that members of staff with Smartcard Registration Authority access to their Clinical Information System use this authority lawfully and in accordance with Confederation policy.
     12. The Confederation will maintain a Business Continuity Plan to assure the continuation of Confederation Hosted Service in the event of adverse incidents or disaster.
  2. In the furtherance of activities within the scope of this agreement, the Practice agrees to the following:
     1. The Practice will comply with the law in all aspects of Data Protection and relevant national guidance including but not limited to:
        1. General Data Protection Regulation 2018
        2. Data Protection Act 2018
        3. Human Rights Act 1998
        4. Privacy and Electronic Communications Regulations 2003
        5. Health and Social Care (National Data Guardian) Act 2018
     2. The Practice will ensure that their staff who access the Confederation Clinical Information System comply with Confederation policies.
     3. The Practice will delegate Registration Authority to the Confederation to assign appropriate smartcard profiles to clinical staff who require access to their Clinical Information System to provide their patients with care.
     4. The Practice will ensure that it meets the minimum standards for Information governance set out in the DSP Toolkit.
     5. The Practice will maintain registration with the Information Commissioner’s Office.
     6. The Practice will ensure that their privacy notice includes:
        1. Details of how their data is stored on the Confederation Clinical System for the purpose of providing services at scale.
        2. Details of how their data is processed by Confederation staff for the purpose of providing care in extended access services.
     7. The Practice will work with the Confederation to investigate and resolve any incidents, complaints or concerns from patients regarding Confederation delivered or hosted services or infrastructure.

Information Governance Standards

* + 1. An objective of this agreement is to provide assurance that all parties will work to the same level of information governance standards.

This is measured through the annual self-assessment audit against the service-specific standards set out in the Data Security and Protection Toolkit or equivalent standard. Non-compliant organisations will have their access revoked and would be required to have formal discussions regarding access.

* + 1. In particular, to support the Framework including the Data Processing and Information Sharing agreements, it is the responsibility of each partner to:
       1. Identify a named individual(s) who takes responsibility for this Agreement on behalf of the partner organisation;
       2. Identify a named individual to act as the organisation’s central point of contact to support the operation of Confederation information systems;
    2. Have procedures and policies in place to ensure:
       1. Staff (including temporary staff, agency staff, secondee’s, contractors, students, placements and volunteers) who have access to Confed systems have been trained and understand their legal and contractual duties for the protection and use of confidential information;
       2. Organisational and technical security measures to protect the integrity, confidentiality and reliability of information on Confederation information systems e.g. via documented access controls, contracts of employment, codes of conduct, information governance policies and education and training programmes;
       3. Information is of a quality fit for the purpose for which it is to be used; including being complete, accurate and up to date, otherwise any decision based on the information may be flawed and inappropriate actions may result;
       4. Policies and procedures are in place to detect, report, investigate and manage personal data breach incidents[[1]](#footnote-1), which include provisions for informing the Information Commissioner’s Office and the data subject(s) as appropriate;
       5. Appropriate Human Resources procedures are in place to deal with staff responsible for a personal data breach incident and all staff are made fully aware of those procedures;
       6. Procedures are in place and published to deal with individual service user’s rights i.e. procedures for dealing with requests for access to personal data, right to information, right to object to certain data sharing, queries and complaints.

## Data Processing Agreement

* 1. This Data Processing Agreement forms part of the Framework Agreement between the Confederation (the Data Processor) and the Practice (the Data Controller), which together will be referred to as ‘the Parties’.
  2. The Practice acts as a Data Controller.
  3. The Practice instructs the Leeds GP Confederation to act as a Data Processor for the purposes of delivering Direct Care to registered patients of the Practice. The Practice instructs the GP Confederation to process data as required to fulfil its duties as defined in the EXTENDED ACCESS Contract.
  4. The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
  5. The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

* 1. **Definitions and Interpretation**

Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

"**Agreement**" means this Data Processing Agreement and all Schedules;

"**Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Practice pursuant to or in connection with the Principal Agreement;

"**Contracted Processor**" means a Subprocessor;

"**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

"**EEA**" means the European Economic Area;

"**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

"**GDPR**" means EU General Data Protection Regulation 2016/679;

"**Data Transfer**" means:

a transfer of Company Personal Data from the Practice to a Contracted Processor; or

an onward transfer of Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

"**Services**" means

The services provided by the Data Processor to, or on behalf of the Practice. "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Practice in connection with the Agreement.

The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

**Processing of Personal Data**

Processor shall:

comply with all applicable Data Protection Laws in the Processing of Personal Data; and

not Process Personal Data other than on relevant instructions by the Practice.

* 1. **Processor Personnel**

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

* 1. **Security**
     1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
     2. In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.
  2. **Subprocessing**

Processor shall not appoint (or disclose any Personal Data to) any Subprocessor unless required or authorized by the Practice.

* 1. **Data Subject Rights**

Taking into account the nature of the Processing, Processor shall assist the Practice by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Practice obligations, as reasonably understood by Practice, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

* + 1. Processor shall:
       1. promptly notify the Practice if it receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and
       2. ensure that it does not respond to that request except on the documented instructions of the Practice or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws
    2. inform the Practice of that legal requirement before the Contracted Processor responds to the request.
  1. **Personal Data Breach**
     1. Processor shall notify the Practice without undue delay upon Processor becoming aware of a Personal Data Breach affecting Personal Data, providing the Practice with sufficient information to allow the Practice to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
     2. Processor shall co-operate with the Practice and take reasonable commercial steps as are directed by the Practice to assist in the investigation, mitigation and remediation of each such Personal Data Breach.
  2. **Data Protection Impact Assessment and Prior Consultation**

Processor shall provide reasonable assistance to the Practice with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Practice reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of the Practice Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

* 1. **Deletion or return of Personal Data**

The Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of the Practice Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Personal Data.

* 1. **Audit rights**
     1. The Processor shall make available to the Practice on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Practice or an auditor mandated by the Practice in relation to the Processing of Personal Data by the Contracted Processors.
     2. Information and audit rights of the Practice only arise to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.
  2. **Data Transfer**

The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Practice. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

* 1. **Confidentiality.**

Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“**Confidential Information**”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

* + - 1. disclosure is required by law;
      2. the relevant information is already in the public domain.
  1. **Notices.**

All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

## Information Sharing Agreement

* 1. Agreement
     1. The agreement is made between the Confederation and the Practice to govern the sharing of information stored on the DATIX© Incident Management system.
     2. The Practice agrees to share information with the Confederation inasmuch as the Confederation complies the arrangements for sharing as set out in this agreement.
     3. The Practice instructs the Confederation to process data held on the Practice on the DATIX© Incident Management System.
  2. Principles
     1. Data should be processed by the Confederation when it is needed for the safe and effective care of the individual.
     2. Parties this Information Sharing Agreement will follow the principles listed in clause 5 of the Leeds GP Confederation Data Security and Protection Framework Agreement.

The Purpose(s) for Information Sharing

* + 1. Information should be processed between the Leeds GP Confederation and the Practice between whom their is a legitimate relationship where it is necessary for the purpose of the “direct care” of patients registered with the Practice.
    2. “Direct care” is defined as a clinical, social, or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals (all activities that contribute to the diagnosis, care and treatment of an individual) [[2]](#footnote-2).

The Types of Information to be processed.

* + 1. Only information contained within the DATIX® Incident Management System will be processed.
    2. Only Information that is necessary, relevant and proportionate to the direct care purpose will be processed.
       1. The GP Confederation will only process data required to effectively and safely manage the services which it provides to registered patients of the Practice including the management of incidents and serious incidents which occur during the delivery of these services, which are logged on the system by GP Confederation staff, Practice staff, or any other staff involved in the delivery of services provided by the GP Confederation.
  1. Patient Confidential Data will not be processed or shared
     1. Data within the system must be anonymised or pseudonymised as appropriate;
     2. The GP Confederation and the Practice should follow the principles in clause 5 of the Leeds GP Confederation Data Security and Protection Framework Agreement in training staff to only record the information required on the DATIX® Incident Management System which is required to effectively and safely manage incidents and serious incidents

Restrictions on the use of Information

* + 1. All information that is processed must only be used where it is necessary, relevant and proportionate for the purpose specified in this agreement.
    2. Exceptions to this are only applicable when the disclosure is mandated by statute or regulation, under the instructions of a court or via obtaining the explicit consent of the service user.
    3. Any further uses made of this data will not be covered by the Agreement and will be in breach of the Agreement and at risk of being unlawful. This would be managed in accordance with each partner organisations local incident management policies and procedures.

Access to information

* + 1. Authorised Staff

Access to the DATIX© system will be provided to health and social care professionals and their teams involved in the provision of direct care to service users and controlled in accordance with NHS Leeds CCG Governance Team access policies and procedures.

The GP Confederation will manage the user access management procedures, including liaising with the CCG to facilitate the registration and de-registration of access, on behalf of the Practice.

Requests for Access Information

* + 1. The procedure for managing requests for information, including requests made under the Freedom of Information Act 2000, will be documented and managed using the GP Confederation FOI Procedure (Appendix v).

Data Protection Legislation

* + 1. Data Controllers
       1. In the terms of the GDPR a Data Controller works alone, jointly or in common with other data controllers, depending on the circumstances of the data processing activity[[3]](#footnote-3).
       2. Each Health and Social Care partner is an individual Data Controller and is alone legally responsible for ensuring their processing of PCD is done fairly and lawfully in compliance with data protection legislation.
       3. Any processing of personal data undertaken by a Data Controller and their staff, is undertaken in their own right and each Data Controller party to this Agreement is not liable for the actions of another.
    2. Data Processor
       1. The Practice is a Data Controller in respect of the personal data held about their patients.
       2. The GP Confederation acts as the Data Processor in respect of their duties in the management of incidents which occur in the services they provide, and the management functions outlined in this document.
    3. Article 28 & 32 GDPR
       1. Article 32 of the GDPR requires an assessment to ensure that the appropriate level of security is applied to the processing of data, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
       2. In particular, where a Data Controller enters into an arrangement with a Data Processor to process personal data on their behalf, that arrangement must be supported by a written contract. Article 28 of the GDPR states processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
          1. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
          2. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
          3. takes all measures required pursuant to Article 32 of the GDPR;
          4. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III of the GDPR;
          5. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the processor;
          6. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
          7. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (vii), the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

Information Sharing Agreement

* + 1. All parties agree to uphold the common law duty of confidentiality, the GDPR and Human Rights Act 1998 and ensure information is shared fairly, lawfully and responsibly in accordance with the Caldicott Principles and NHS Confidentiality Code of Practice.
    2. All parties agree to publish this agreement in addition to other fair processing information to support openness and transparency.[[4]](#footnote-4)
    3. All parties agree to work together to establish and implement technical and organisational policies and procedures that support the sharing of information in accordance with this Agreement.

Responsibility for this Agreement

* + 1. Each partner takes responsibility for ensuring the application of the terms and conditions of this Agreement within their organisation.
    2. The Quality, Finance and Performance Committee will take responsibility for ensuring the overall management of this Agreement, including its continual monitoring, revision and updates.
    3. Additional supporting materials, such as policy, procedure or subsequent amendments to this Agreement will only be approved by the Quality, Performance and Finance Committee following consultation with all signatory partner organisations and issued as agreed supplementary appendices.
    4. This Agreement will be subject to a formal annual review by the Quality, Performance and Finance Committee, taking into consideration:
       1. non-compliance issues with this Agreement, logged and reported by any party (including complaints arising from information sharing);
       2. non-compliance with any supplemental policies, procedures and guidelines, logged and reported by any party (including complaints arising from information sharing);
       3. any general difficulties encountered in applying this Agreement, logged and reported by any party.

An earlier review may be necessary to take changes in the law and/or national policy into account.

## Smartcard Registration Authority Agreement

* 1. Introduction

A Registration Authority (RA) is the governance framework within which NHS organisations can register individuals as users of the NHS Care Records Service and other services - maintaining the confidentiality and security of patient information at all times.

Registration is the process by which users who require access to Smartcard-enabled IT applications are authenticated (proven who they are beyond reasonable doubt) and authorised (enabled to have particular levels of access to particular patient data and systems).

Local NHS England Regional Teams are responsible for commissioning local ‘Registration Authorities’ (RAs) services.

Aims

This agreement aims to set out the framework within which the Leeds GP confederation will work with the Practice to ensure that Registration Authority processes, including the granting of RA sponsor roles and other smartcard access profiles to staff who care for their patients, are sufficient to ensure access to medical records is controlled and limited to the purpose of providing direct care.

Scope

This policy must be followed by all staff who work for or on behalf of the Leeds GP Confederation, or the Practice including those on temporary or honorary contracts, secondments, volunteers, pool staff, Governing Body members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the Practice. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

Accountability and Responsibilities

There are a number of key information governance roles and bodies that the GP Confederation has in place as part of its Information Governance Framework, these are:

The Executive

Quality Performance and Finance Committee

Caldicott Guardian

Head of Governance

Information Asset Owner/Administrator

Heads of Service/department

All employees

* + 1. Responsibilities of the GP Confederation

The GP Confederation is responsible for ensuring that any staff acting on its behalf and working in the capacity of RA Sponsor for the Practice works according to the provisions set out in clause 5 of the Leeds GP Confederation Data Security and Protection Framework Agreement.

The GP Confederation will follow the operating procedures set out in Appendix xii to obtain RA Sponsor status for any staff working on its behalf.

Agreement

* + 1. All parties agree to uphold the principles and provisions of this agreement and those listed in clause 5 of the Leeds GP Confederation Data Security and Protection Framework Agreement.
    2. All parties agree to support the other in delivering care to registered patients of the Practice, subject to the provisions of this agreement and the service contracts held by the Leeds GP Confederation.

## Signatures

This Agreement shall be signed on behalf of each party by its Caldicott Guardian.

This Agreement will be published in accordance with the terms of the Freedom of Information Act 2000.

This Agreement may be executed in counterparts, each of which shall be deemed to be an original document but all of which taken together shall constitute one single agreement between the Parties.

**On behalf of the Leeds GP Confederation the following authorised signatories agree to the terms set out in this Agreement:**

**Name:** Dr Ruth Burnett

**Designation:** Medical Director, Caldicott Guardian

**Signature: Date:**

**Organisation Address:** The Leeds GP Confederation, 2nd Floor Stockdale House, Leeds, LS6 1PF

**The following person will act as the organisation’s central point of contact for matters concerning this Agreement:**

**Name:** Simon Boycott, Head of Development and Governance

**Contact details:** The Leeds GP Confederation, 2nd Floor Stockdale House, Leeds, LS6 1PF

**Email:** simon.boycott@nhs.net

**Telephone:** 0113 843 0785

**On behalf of the Practice the following authorised signatories agree to the terms set out in this Agreement:**

**Name:**

**Designation:**

**Practice:**

**Signature: Date:**

**Practice Address:**

**The following person will act as the organisation’s central point of contact for matters concerning this Agreement:**

**Name and Designation:**

**Contact details:**

**Email:**

**Telephone:**

Appendix i. Hosted Services Agreement

Arm’s Length Hosted Service Agreement

This is an agreement between the [insert name of PCN] Primary Care Network and Leeds GP Confederation for Arm’s Length Hosting of Hub Services on Leeds GP Confederation Clinical System.

This agreement is to enable Networks to set up and manage Network services or shared booking rotas considered outside the Extended Access remit and may include initiatives such as shared wound care clinics, shared visiting rotas, shared pharmacy clinics for AF or Frailty, shared Carer clinics, shared clinics to support QIS work streams.

**Roles and Responsibilities**

**Primary Care Network:**

* Initiating within reasonable timeframe discussion with Confed Ops team re new staff, clinics and roles and organising set-up meeting
* Application forms completed and send to Confed for Network staff and any new staff member needing to hold clinic on Hub
* Nominating staff for management of rotas – signed agreement
* Organising suitable training for any staff using rotas on hub – through GP Confed team
* All arrangements relating to the access to Network clinical systems for staff who need to access patient records and all responsibilities as part of this including IG responsibilities - see process for full details
* Ongoing management of rotas for Network specific services/clinics
* Informing GP Confed colleagues of any changes to staff roles – leavers for Hub Quarterly or sooner
* Ensuring that each practice in the PCN who will access the Clinical System has signed the Leeds GP Confederation Data Security and Protection Framework Agreement

**GP Confederation Ops team responsibilities**

* Meet with Network for set up discussion and advice and where needed adding new USER for rota
* Training for staff to ensure competency around managing rotas on hub
* Training for staff holding rotas on Hub on general navigation and operation
* Adding appropriate staff to hub with appropriate access rights – timely
* Removal of admin rights where Network communicated leaver etc
* Ensuring compliance of Staff with the Leeds GP Confederation IG Policy and Framework

**Primary Care Network nominated Rota manager/s with additional GP Federation Hub rights**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Job role: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Smartcard UUID : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employing practice/org: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Already has Hub access: Yes /No – Authorising practice if Yes \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(If No – standard Hub paperwork is also needed)

Training session with GP Confederation Ops staff held: Yes/No/Planned for:\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Job role: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Smartcard UUID :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employing practice/org: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Already has Hub access: Yes /No – Authorising practice if Yes \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(If No – standard Hub paperwork is also needed)

Training session with GP Confederation Ops staff held: Yes/No/Planned for:\_\_\_\_\_\_\_\_\_\_\_\_\_

**The [insert name of PCN] Primary Care Network agrees to the formal nomination and roles as outlined in this agreement and understands that this can be reviewed/revoked if the Agreement is not fully complied with by either Network or GP Confederation.**

**Primary Care Network Locality Manager**:

Signed : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Arms Length Hosted Services Arrangements between GP Confederation and PC Network to offer clinics on Hub: Process**

**Initial set up**: The Network agrees to an initial consultation conversation with colleagues from GP Confederation Ops team either face to face or over telephone to ensure that any proposed new Branches, new clinic types or roles, rotas and slot types are agreed as appropriate with the GP Confederation Operational Team at earliest opportunity before new projects/staff begin: (for example new OT project, new shared wound care clinic, ) this is an opportunity to ensure naming and use of Branches rotas and slot types does not cause confusion and set up is considered from citywide perspective. Booking of training session for staff operating for Network can be agreed at this meeting.

**Nominated Staff for rota management**: The Primary Care Network has a nominated staff member/s (listed in agreement who will take responsibility for publishing and maintaining locally owned rotas and this staff member has a training session with GP Confederation Hub colleagues to ensure they understand the Hub set-up, configuration, limitations and restrictions at the point that their access is granted/extended. This staff member had additional access rights to hub including amending and publishing rotas.

**Hub Access Application Process**: The Network enrols any new clinical staff member/s who needs access to the booking platform onto the Hub using the standard GP Confed IG forms and providing required IG documentation. – this part is enabled by GP Confederation staff as per normal procedure for a new staff member being able to book and view appointments on Hub.

**Network Staff Operating clinics on the Hub:** The staff member if not already inducted into the GP Confed Hub is booked a training session with GP Confed Ops team to ensure they understand the different process around navigating the Hub compared to standard S1 units, the branch set up and have appointment set up configured with bookmarks, the process for arriving and marking patients as seen in rotas.

**Practice Clinical System access for Shared Network clinical staff**: The Network takes full responsibility for ensuring any Network staff operating shared clinics have access to the required practice level units to be able to see patients booked onto the Hub with appropriate access to the full clinical record– they do this with the agreement of Network practices and take responsibility for:

* enabling smartcard access and advising on appropriate staff roles at practice level
* configuring templates/clinical trees for staff
* ensuring access works correctly at each unit before clinics are published.
* Ensuring clinical staff are appropriately trained in use of any practice clinical system (This may include booking staff onto Staff training on basic S1/EMIS use which is available through normal CCG Channels. See Data Quality team).
* Ensuring documents in place as evidence of IG training and maintaining adequate record of Network staff and forms / agreements / IG training dates etc – recommended spreadsheet fields attached to be held at Network level.
* Ensuring any staff leaving Network roles are communicated to GP Confederation for removal from Hub and Network practices at earliest opportunity
* Picking up any IG issues, complaint and overseeing IG compliance and any investigation into IG breeches.

**Rotas and Appointments** : the Network maintains all rotas for Shared network clinics outwith the Extended Access provision, is responsible for the cancelling or amending of any clinics and cascading such information to Network practices

**Non Standard NHS roles**: The Network agrees NOT to propose any staff member on behalf of the Network without recognised NHS role for access to the GP Confederation hub appointment system through the standard process. Requests to add staff roles which are not traditionally NHS roles such as ie DWP Colleagues, Carers Leeds, Healthy Lifestyle Services –must be made through a separate proposal with decisions on granting access to the Hub made on a case by case basis with the opportunity for agreement at Leeds Extended Access Steering board. Alternative solutions to granting these staff access may be proposed including providing staff with a specific clinic list rather than full access to the Hub.

Recommended -spreadsheet to be maintained by Primary Care Network for IG Audit Purposes

* Shared staff names
* Staff role in network
* Smartcard number
* GP Confed Hub Access Y/N
* Network practice access – listed practices
* Nursing PIN where applicable
* Employment and DBS responsibility (ie Practice name/confed??/other org etc)
* IG Certficate checked and on record
* Date IG training due for renewal
* Start date Network role
* Leave date and any notes – including practice and GP confed notification

**Documents to be held at Network level:**

* IG certificates - copy
* IG form for Hub/other units - copy
* DBS if employed at Network level – or understanding of employee practice/org responsibility
* Staff References if employed at Network level – or understanding of employee practice/org responsibility

**Also recommended**:

Standard Operating Procedure or MoU for services/clinics held at Network level such as Wound Care clinics including procedures around sickness and absence reporting and escalation, criteria for appts and allocation, expectation of clinic continuity in event of cancellation, host practice responsibilities etc

Appendix ii. Leeds GP Confederation Information Governance Policy and Framework



Appendix iii. Leeds GP Confederation Confidentiality Code of Conduct



Appendix iv. Leeds GP Confederation Data Protection Policy



Appendix v. Leeds GP Confederation FOI Procedure



Appendix vi. Leeds GP Confederation Information Handling Policy



Appendix vii. Leeds GP Confederation Network Security Policy



Appendix viii. Leeds GP Confederation Individual Rights and SAR Procedure



Appendix ix. Leeds GP Confederation Incident Management and Serious Incident Policy



Appendix x. Leeds GP Confederation Records Management Policy



Appendix xi. Registration Authority Services Supporting Information

General Practices can use the following list to find their local RA contact:

[**List of RA contact details**](https://digital.nhs.uk/services/registration-authorities-and-smartcards/primary-care-service-provider-contact-details)

Where information is missing or incorrect you may obtain RA contact information from your local NHS England Regional Team

RA standards and processes:

National RA operating guidance was published by HSCIC to assist local NHS England teams and LPCs to ensure that RAs are meeting appropriate standards.

Although the RA has ultimate responsibility for smartcards matters, most day to day smartcard management ca be carried out by the Practice using the [**Care Identity Service (CIS)**](https://portal.national.ncrs.nhs.uk/portal).

[**NHS Digital has produced comprehensive guidance for users in relation to this tool.**](https://digital.nhs.uk/services/registration-authorities-and-smartcards/care-identity-service)

Smartcard Roles in General Practice

There are several reasons for Smartcard use in General Practice, many of which will facilitate general use of the General Practice Clinical System and allow staff members to access the Clinical System.

Appropriate ‘roles’ are applied to Smartcards so General Practice team members can carry out the tasks and duties relevant to their job.

In addition, there are two roles that can be assigned to a General Practice staff members’ Smartcard so they can help other General Practice team members with Smartcard matters.

Both roles are slightly different and each ‘role’ controls what a General Practice team member can do and what they can see. The intention is to preserve patient safety and confidentiality.

These roles are:

Local Smartcard Administrator (LSA): A LSA can use the Care Identity Service (CIS) to assist with unlocking and renewing a Smartcard.

Sponsor: A Sponsor can use CIS to assist with unlocking and renewing a Smartcard. In addition, they can raise a request to have a new member of General Practice staff registered for a smartcard and raise a request to change a role.

Becoming an LSA/Sponsor

LSA’s/Sponsors require:

a functioning Smartcard

two Smartcard readers at the Sponsor’s General Practice premises

understanding of the responsibilities and obligations involved;

appropriate training

RA approval.

Sponsor responsibilities

Familiarity with:

Care Identity Service (CIS)

Roles: Be familiar with the different types of access profiles / CIS positions to approve, and how to support other processes associated with cards.

Scope of their sponsor role: Understand which user registrations they can support within the scope of the authority granted to them

Local RA methods: Be aware of the method the local RA use to follow national guidelines and requirements. Sponsors will work with their local RA to maintain access to NHS CRS compliant systems within their area of responsibility consistent with the NHS Confidentiality Code of Practice and Care Record Guarantee.

Temporary Access Card arrangements.

Identity checks by Sponsors

Sponsors must be assured of the identity for users they sponsor.

The sponsor needs to be assured that the user’s identity has been confirmed beyond reasonable doubt and that the user requires the level of access requested and need to confirm with that the individual requires the requested level of access.

Care Identity Service (CIS)

The software system used to administer Smartcards is known as the [**Care Identity Service (CIS).**](https://portal.national.ncrs.nhs.uk/portal)

Uses

It is used to apply the appropriate level of access to General Practice staff (and other healthcare professionals) who need access to clinical systems by issuing them with an individual Smartcard and the appropriate role on that Smartcard. The system can also be used to unlock and renew Smartcards, update passcodes and the General Practice staff contact details.

Local Smartcard Administrators, Sponsors and other RA staff, for example, the RA Manager, RA Agents, RA Agents Advanced (who will predominantly sit at the RA Service Provider Organisation) will also use CIS to administer card matters.

Using the CIS can be selected from [**NHS Spine Portal**](https://portal.national.ncrs.nhs.uk/portal): (Smartcard required).

[**NHS Digital has produced comprehensive guidance for users in relation to this tool.**](https://digital.nhs.uk/services/registration-authorities-and-smartcards/care-identity-service)

Settings

Where you cannot access the Spine portal, this may relate to software/Java settings and therefore IT helpdesk should be contacted (e.g. their IT department if they have one, and/or their system supplier) to ensure their system is setup to run CIS as well as all of the other programmes the General Practice will need.

Prerequisites

The Practice network has to be configured to allow access to the NHS Spine Portal. Therefore, systems have to be able to connect with the following Spine Portal IP addresses:

<https://portal.national.ncrs.nhs.uk/portal>

<https://portal2.national.ncrs.nhs.uk/portal>

<https://uim.national.ncrs.nhs.uk/portal>

Appendix xii. Standard Operating Procedure for Hub Staff Registration



Appendix xiii. Standard Operating Procedure for Extended Access Staff Induction



1. The Independent Information Governance Review Panel recommended the term “personal data breach incident” to be used as the standard term for health and social care services to cover ‘data losses’, ‘personal data breaches’ and ‘information governance serious incidents’ etc. See Glossary. [↑](#footnote-ref-1)
2. Health and Social Care Information Centre Confidentiality Guidance for Health and Social Care - references [↑](#footnote-ref-2)
3. DPA Part 1 Section 4(4) [↑](#footnote-ref-3)
4. Fair processing is a requirement of the first DPA principle (fair and lawful). [↑](#footnote-ref-4)