

**Local Health and Care Records**

**Information Governance Framework for Integrated Health and Care**

**(Assurance version for journey 1 only - updated)**

cid:image002.png@01D4D8D2.62F37080**NHS England and NHS Improvement**

**Information Governance Framework for Integrated Health and Care (Assurance version for journey 1 only - updated)**

Version number: v0.9 – 31st May 2019

First published: n/a

Updated: n/a

Prepared by: Dawn Monaghan, Head of Data Sharing and Privacy (NHS England)

Classification: (Official)

Thank you to colleagues from the LHCR IG Steering Group, LHCR IG Leads and critical friends who have helped in the development of this document.

# Contents

[Contents 3](#_Toc10223043)

[Executive Summary 5](#_Toc10223044)

[1. Introduction 7](#_Toc10223045)

[2. Using the Information Governance Framework 8](#_Toc10223046)

[2.1 Secondary Use Data Governance Tool 8](#_Toc10223047)

[3. General Principles 9](#_Toc10223048)

[4. Requirements 10](#_Toc10223049)

[4.1 The Importance of Good Information Governance Practice for LHCRs 10](#_Toc10223050)

[4.2 Understanding Legal Requirements 11](#_Toc10223051)

[4.2.1 Statutory duties and functions 12](#_Toc10223052)

[4.2.2 Data Protection Act (DPA) 2018 /GDPR 12](#_Toc10223053)

[4.2.3 Common Law Duty of Confidentiality 13](#_Toc10223054)

[4.2.4 Meeting the Human Rights Act obligations 14](#_Toc10223055)

[4.2.5 The Duty of Transparency 15](#_Toc10223056)

[4.3 Determining data flows and controllership 17](#_Toc10223057)

[4.3.1 Joint Controllership 18](#_Toc10223058)

[4.3.2 Data sharing arrangements 19](#_Toc10223059)

[4.4 Records of Processing Activity Art.30 20](#_Toc10223060)

[4.5 Assuring security 21](#_Toc10223061)

[4.5.1 Using Processors 21](#_Toc10223062)

[4.5.2 The Data Security and Protection Toolkit (DSPT) 22](#_Toc10223063)

[4.5.3 Data and Cyber Security Standards 22](#_Toc10223064)

[4.5.4 Effective Cyber Threat Situational Awareness 22](#_Toc10223065)

[4.6 Data Access, Review and Retention 23](#_Toc10223066)

[4.7 Individual Rights 24](#_Toc10223067)

[4.8 Patient Objection to Processing and National Data Opt-Out 25](#_Toc10223068)

[4.8.1 National data opt-out 25](#_Toc10223069)

[4.8.2 Patient Objection to Processing 26](#_Toc10223070)

[4.9 Demonstrating Accountability 28](#_Toc10223071)

[4.9.1 Adopting principles by design and default 28](#_Toc10223072)

[4.9.2 Data Protection Impact Assessments (DPIA) 28](#_Toc10223073)

[5. Journey 1 – Individual care within a LHCR (between health and social care bodies) 30](#_Toc10223074)

[6. Journey 2 – Individual Care Across Geographical LHCR Boundaries 31](#_Toc10223075)

[7. Journey 3 – Improving health, care and services through planning and evaluation (Secondary Uses/Population Health Management) 33](#_Toc10223076)

[8. Journey 4 – Research 37](#_Toc10223077)

[Appendices 39](#_Toc10223078)

[Appendix A - Glossary for the Information Governance Framework 39](#_Toc10223079)

[Appendix B – Using Health Data 46](#_Toc10223080)

[Appendix C - Governance Process 48](#_Toc10223081)

[Appendix D – Definitions of Individual/Direct and Indirect Care 49](#_Toc10223082)

[Appendix E – Lawful Conditions for Processing 50](#_Toc10223083)

[Appendix F – Common Law 54](#_Toc10223084)

[Appendix G - Consent and applicable GDPR Recitals 55](#_Toc10223085)

[Appendix H – Supporting Tools and Templates 56](#_Toc10223086)

[Appendix I – GDPR Article 21 – Right to Object 57](#_Toc10223087)

[Appendix J – GDPR Article 26 – Joint Controllers 58](#_Toc10223088)

[Appendix K – Security Requirements 60](#_Toc10223089)

[Appendix L - 2017/19 NHS Standard Contract 61](#_Toc10223090)

[Appendix M - Assurance Checkpoint Matrix (for completion by the LHCREs) 62](#_Toc10223091)

[Appendix N - Individual Rights under GDPR - Art. 12 - 23 67](#_Toc10223092)

[Appendix O – Data Breach Management 70](#_Toc10223093)

[Appendix P – Role Based Access Control (RBAC) 72](#_Toc10223094)

[Appendix Q – Patient Preferences Template Text 75](#_Toc10223095)

# Executive Summary

The aim of the Local Health and Care Record (LHCR) programme is to help local organisations move from today's position where each health and care organisation holds separate records for the individuals they care for, to one where an individual's records are connected from across the health and care system.

This will help health and care professionals to share information safely and securely as the people they care for move between different parts of the NHS and social care. It will also enable individuals to be able to access their record irrespective of which part of the health and care system that has provided them care.

The content of the core record will be based on professionally agreed standards developed by the Professional Records Standards Body (PRSB). Professionals across a wider range of different sectors, as well as patients and carers, have informed what and how information should be recorded at various points of care, from birth, through life events, maternity and end of life.

The approach recognises the variance that we currently have in how data is captured and represented in local systems. The LHCR record will assist care professionals by bringing together content that can be standardised and then consistently displayed for example by providing a consolidated medication list.

This national Information Governance Framework provides a structured approach to ensure LHCR participants meet their legal obligations when planning, preparing and delivering data sharing. It is based on a model where data controllership continues to remain local. This means local agreements will be in place to set out what data is shared and who can access this data so that this is done in a safe, secure and appropriate manner.

The LHCR programme has been broken down into down into four “journeys”. These are:

* **Journey 1 – Sharing personal/confidential patient information (CPI) between health and social care bodies within a LHCR for the individual care[[1]](#footnote-2) of patients and service users**. The Long-Term Plan sets out a commitment to provide national coverage of LHCRs and therefore the intention is that there would be a record for each member of the population.
* **Journey 2 – Sharing personal/confidential patient Information (CPI) between health and social care bodies across geographical boundaries for the individual care of patients**. A patient's LHCR area will be determined by where their GP practice is based. However it is important that information is available at the point of care for a patient. A requirement of LHCRs is that there is the ability to share information with other LHCRs.
* **Journey 3 - Sharing personal/confidential patient information and anonymous data between health and social care bodies within a LHCR and across LCHR geographical boundaries to improve health, care and services through planning**
* **Journey 4 - Sharing personal/confidential patient information and anonymous data with others for health and care research purposes (Research)**

The Information Governance Framework will enable the processing of data in an appropriate and transparent manner. It will support LHCRs to ensure that data sharing complies with statute; common law; the values set out in the NHS Constitution and enshrined in the provision of social care; and professional guidelines on sharing information as set out for health and care staff.

This guidance has been designed as comprehensive but practical guidance, which enables all participants (data controllers) in the LHCR programme to meet their information governance responsibilities. It is principally written for information governance professionals although it will be helpful for all those who are involved in using patient information generated by individual LHCRs. It provides advice around some of the complex areas, which will apply to LHCRs such as joint data controllership and considering patients’ choices about how their data is used. It also provides practical tools and templates for organisations to use.

This is all provided in a way that is designed to be of immediate, practical help to the LHCRs to improve their information governance and build trust with the people they serve. The framework is expected to be a working document and will evolve over time to meet the needs of those who use it, taking account of operational experience and reflecting any changes to policy, technology and the law.

DN - Expand on each journey to include details of end points and include what the framework is not (1.11.3)

# 1. Introduction

The invitation to participate[[2]](#footnote-3) in the LHCR programme promised*: “This will all be undertaken within a consistent national framework of information governance which will assist exemplars to meet their legal obligations'*

As part of the bidding process, local areas were asked to submit details of their current information governance arrangements, including the steps they have taken to ensure compliance with the law and maintain high standards of data security. This revealed much evidence of good practice, but also room for improvement, even among those whose bids were successful.

It is essential that innovative ways of working are tested against relevant law and guidance including the data protection legislation (General Data Protection Regulation [GDPR] and the Data Protection Act 2018) and the Common Law Duty of Confidence. While individual LHCRs will reflect local priorities and differences, there will need to be a consistent national approach to information governance considerations involved in establishing and operating a LHCR. This will support, build and maintain public trust and confidence. The Information Governance Framework will provide a clear, coherent, compliant and accountable approach to the use of health and social care data even if the delivery mechanisms and systems are different.

In association with this IG Framework technical documents are being prepared which will include authentication, audit, protection of APIs, redaction, handling patient objections to sharing and other enabling security functions.

# 2. Using the Information Governance Framework

This Framework begins with general principles, which will apply to all four journeys. These are followed by a set of requirements for each journey with which LHCRs will need to comply; there is an assurance checkpoint to assess attainment. A self-assessment Assurance Matrix is available at Appendix M for LHCRs to complete for submission to the external IG Assurance Panel as part of the assurance process.  LHCRs need to achieve satisfactory assurance on each checkpoint and be fully compliant across all checkpoints for Journey 1 by March 2020.  Where a LHCR already has a shared local health and care record in place they should use the Matrix to assure themselves and the assurance panel that they are compliant.  In the event that satisfactory assurance cannot be met support will be provided to achieve compliance.

Many existing LHCR member organisations already have mature systems, which aid the delivery of information governance commitments and requirements. It is anticipated that these local delivery systems will continue and must be externally assured to ensure consistency with this Framework. As part of the LHCR Information Governance Leads Network, good practice from local systems should be shared and capitalised upon.

## 2.1 Secondary Use Data Governance Tool

The Secondary Use Data Governance Tool (SUDGT) has been developed by NHS England to support Sustainable Transformation Partnerships/Integrated Care Systems (STPs/ICSs) to implement robust governance processes to support their use of data, focused on data required for secondary purposes (see Appendix H for link).

The SUDGT includes a matrices document, which lists the statutory duty/lawful basis for processing for each organisation type, mapped to the type of activities, which need to be undertaken to meet them. It maps these to the type of data which may be required. It also proposes contractual and data processing models to enable delegation of the activities required to meet the data controller’s secondary purposes. Use of the SUDGT considers and builds upon the legal and governance considerations required for compliance and assurance with data protection and privacy.

The tool forms the basis of journey 3 (secondary use purposes) however users may find this a useful tool across other journeys.

# 3. General Principles

The following principles should be applied by LHCRs to support improved access to data, streamline data sharing pathways and meet legal accountability obligations:

1. Demonstrating compliance with the law by:

* Identifying lawful justifications for processing information
* Ensuring transparency about purpose and process
* Minimising the use of identifiable data
* Ensuring the use of data protection by design and default
* Promoting the application of appropriate technical and organisation measures
* Adhering to the National Data Guardian’s 10 data security standards [[3]](#footnote-4)
* Mapping data flows and determining roles and responsibilities
* Introducing standards and controls for de-identification and the risk mitigation of re-identification to protect people’s identities (see journeys 3 & 4)

All of the above should be within a Data Protection Impact Assessment (DPIA).

1. This guidance promotes and should reduce unnecessary burden and bureaucracy by providing appropriate tools, templates and models.
2. Supporting best practice and promoting public engagement

# 4. Requirements

The following requirements are essential for LHCR information governance compliance and good practice and need to be considered for all journeys.

## 4.1 The Importance of Good Information Governance Practice for LHCRs

The General Data Protection Regulation (GDPR) stipulates the requirements for controllers and processors and where there is a requirement to have a Data Protection Officer (DPO) in place. In addition all NHS organisations and local authorities, which provide social services must have a Caldicott Guardian. A Caldicott Guardian is a senior person responsible for protecting the confidentiality of health and care information. They should normally be a senior health professional or be closely supported by such a person.  It is important that health and care professionals are represented in discussions.  This is particularly important in relation to processes, for example to ensure that IG decisions do not have unintended burden consequences or to ensure that a clinical view is factored into processes such as when dealing with Subject Access Requests or considering whether to uphold a patient’s objection/withdrawal of consent to the sharing of their data/information.

Each LHCR will need a consistent approach to information governance policies, processes and systems to ensure good practice across the LHCR. To achieve this, one individual will need to take the lead for a LHCR’s information governance approach and work with their information governance colleagues within the LHCR’s constituent organisations. The LHCR Accountable Officers should decide which information governance representative takes the role of Information Governance Lead. They will need to be a subject matter expert and they are likely to be a Data Protection Officer (although this will not necessarily be the case in every LCHR).

The LHCR Information Governance Lead should be a senior post with the power to make sure that information governance policies are implemented. The LHCR Information Governance Lead, should implement a communications channel with information governance representatives in each of the LHCR organisations, should represent their colleagues, provide a conduit for communications and become part of a LHCR information governance network who meet on a regular basis. Representation from the network will also be required at the national strategic information governance meetings. The Information Governance Lead will also be required to work with Caldicott Guardians, as well as local information governance staff.

Organisations must ensure information governance resource is planned and budgeted for to meet the requirements set out above for an information governance function. It is hoped that some national support for operational information governance may be made available through local Commissioning Support Units (CSUs).

For tools and templates to support this section please see Appendix H (4.1).

|  |
| --- |
| **Assurance Checkpoint**   * Appointment of a LHCR Information Governance Lead * LHCR Information Governance Lead is a member of the LHCR Information Governance Leads network and attends national strategic Information governance meetings * Structure chart for LHCR information governance and communication input * Evidence of information governance Policies |

## 4.2 Understanding Legal Requirements

It is important that each LHCR identifies and understands its legal basis for processing data for every function carried out by the LHCR. The legal basis and information governance rules may change depending on the purpose for which the data is used, therefore when starting a new initiative, the following steps are required:

Determine the purpose/s for which the data will be used;

* Complete a Data Protection Impact Assessment for each purpose. This can help explain the rationale behind the proposed purpose.
* Decide which data types will be shared;
* Establish whether that sort of data can legally be used for those purposes by the organisation/s who wish to process the data; and
* Be clear that the public would reasonably expect that sort of data to be used for that purpose

Where there is joint working between organisations such as a LHCR, there is no one legal entity. Hence each organisation has its own legal responsibilities as a controller and will require its own legal basis for the processing. GDPR Article 26 (Joint Controllers) details how joint controller arrangements must be set out and how these liabilities and responsibilities for compliance are allocated, managed and if necessary indemnified for further information on Joint Controllers see 4.3.1 and Appendix J.

There are 5 consistent legal parameters which must be considered when sharing personal/confidential patient information for any purpose:

* Statutory Duties and Functions
* Data Protection Act 2018 (GDPR) lawfulness for processing
* Common Law duty of Confidence
* Human Rights Act obligations
* Health and Social Care Act 2012
* Health and Social Care (Quality & Safety) Act 2015

The following can help assist in deciding whether the processing will be lawful:

### Statutory duties and functions

This is often referred to as *intra vires*. If you are a public body, does the processing you wish to undertake match your statutory functions? In answering this question identify and document the statutory function and the legislation it is derived from (see appendix H (4.2)).

For example:

* Clinical Commissioning Groups (CCGs) and NHS England have a duty to commission health services but this does not confer an automatic power to process personal/confidential patient information for their commissioning purposes.

* Where a Local Authority commissions an NHS agency (The Provider) to deliver its Child and Adolescent Mental Health Services (CAMHS) using the NHS Standard Contract, the Local Authority still retains its duty to respond to statutory complaints (see Appendix L for details).

### 4.2.2 Data Protection Act (DPA) 2018 /GDPR

It is important that the implications of GDPR Article 6, 9 and the DPA are considered to ensure that data sharing meets the legal requirements. Chapter 2 of the DPA is relevant to most processing of personal data and includes the types of processing of personal data to which the GDPR applies and therefore it is important that the GDPR and DPA are read side by side. Each LHCR should be transparent about the legal basis they are relying on for each purpose for which they process data.

In addition, when processing any special category data (such as health information) controllers will also need to identify a separate condition for processing as described in GDPR Article 9 (See Appendix E and Appendix H [4.2]).

**Do not use consent as a condition for processing to meet GDPR/DPA requirements, unless in exceptional circumstances.[[4]](#footnote-5) The most appropriate basis for lawful processing that is available to publicly funded and/or statutory health and social care organisations in the delivery of their functions is Article 6(1)(c)[[5]](#footnote-6) or (e) and Article 9(2)(h) special category data (see Appendix E for further explanation). Where independent care providers are processing personal data in connection with the provision of self-funded care they can rely on Article 6(1)(f) (legitimate interests). There is no change to the Article 9 basis.**

This means that in practice, for much of the data processed in healthcare settings such as GP practices, pharmacies, hospitals, dentists there will be a two-stage process: the first stage giving the lawful basis as applied to all personal data (Article 6 of the GDPR), and the second because you are processing a special category of personal data, data concerning health (Article 9).

First stage: Generally, many healthcare settings including those listed above have a lawful basis for processing personal data because it is necessary ‘for the performance of a task carried out in the public interest’. In some circumstances, the data controllers at the healthcare settings could also say that the processing is necessary for ‘compliance with a legal obligation’ where they have one to provide care, or ‘for the performance of a contract’ (locally commissioned services) or ‘to protect the vital interests of the data subject’ (emergencies). The lawful basis for processing must be recorded.

Second stage: Special categories of personal data, including data concerning health, may be processed only for reasons specified in Article 9 of the GDPR. In the case of most healthcare settings, the reasons are generally for ‘the provision of health care or treatment’ or ‘the management of health care systems or services or social care systems or services’ or ‘necessary for reasons of public health in the area of public health’. When processed for these reasons, a healthcare professional, social work professional or a person with a duty of confidentiality under a legal provision, must be responsible for the processing.

Where processing data and citing Article 6(1)(e) as the basis for processing, you must be able to specify the Act of Parliament, Regulation or Statutory Instrument that provides the lawful basis for the activity. This, in turn, will engage Article 6(1)(e), and provide a lawful basis for processing data.

Should specific processing arise in which explicit consent is required by law, e.g. Human Fertilisation and Embryology Act 2008 and Gender Recognition Act 2004 then please refer to Appendix G.

A flowchart covering Data Protection Requirements has been added to the Tools and Templates [4.1].

### 4.2.3 Common Law Duty of Confidentiality

The Common Law Duty of Confidentiality (CLDC) will need to beconsidered for each journey.

The Health and Social Care (Quality and Safety) Act 2015 inserts section 251B into the Health and Social Care Act 2012. The section places an obligation on a ‘relevant person’, (i.e. a health or adult social care commissioner or provider, hence it is a corporate duty not an individual’s) to share information to facilitate the provision of health and social care services or because they feel it is in the individual’s best interest and accords with the Caldicott 7th principle (see Appendix B). However, this need not be complied with should the relevant person reasonably consider that the individual would object (or be likely to object) to the disclosure of the information. An objection can be raised and considered but does not have to be upheld should the purpose of sharing be justified (see section on patient objections).

In delivering individual care, it is reasonable to rely upon implied consent as the basis for sharing relevant information about their treatment and care needs with others involved in the delivery of their direct care. Unlike the high threshold for consent (where applicable) under GDPR, the same standard of consent is not necessary to satisfy CLDC. Consent under the CLDC may therefore be implied irrespective of the sensitivity of data involved – unless the patient specifically objects to confidential patient information being shared for these purposes.

This approach requires transparency (which is a mandatory requirement under GDPR) and the need to ensure that patients are as informed as possible: for example, through discussions with clinicians, information leaflets, and comprehensive privacy notices (See Appendix F).

**De-identification of data**

When a LHCR requires identifiable data to be processed to render it anonymous they are required to use NHS Digital to process the data for de-identification and therefore can be confident they are meeting legal and technical requirements.

If organisations are to carry out this type of processing outside of the LCHR programme they should be mindful of how they can meet their legal obligations. While GDPR compliance can be achieved, there are likely to be issues around breaching confidentiality if the confidential patient information is sent to a third party for de-identification. These implications of where identifiable data should and can be processed to ensure it is anonymous are under review.

**Using de-identified data**

Data which has undergone a pseudonymising technique can be dynamic depending upon circumstance and the technical and organisational controls in place. The factors which will determine the status of the data, and therefore when information will need to be treated in line with legislative frameworks is presently under discussion.

A flowchart covering Confidentiality Requirements has been added to the Tools and Templates [4.2].

### 4.2.4 Meeting the Human Rights Act obligations

Article 8 of the Human Rights Act gives individuals a right to respect for their private and family life. However, this does not make it unlawful for organisations to process personal data where there is otherwise a lawful basis to do so. If you are a public authority abiding by GDPR and the Duty of Confidence relating to confidential patient information, then it is likely you will meet your Human Rights Act obligations as GDPR’s overarching aim is the protection of the rights and freedoms of individuals where it concerns the handling of their personal data. However, it will be important to ensure that any information sharing is necessary for the specified purpose AND proportionate.

A Data Protection Impact Assessment (DPIA) must be completed at an early stage to identify any risks to the processing of personal data. For further information regarding DPIA see section 4.9.2.

While many patients and service users are supportive of activities such as clinical research, disease registration and service planning it is wrong to assume that they would be content for personal/confidential patient information to be shared for these purposes without their explicit consent or another legal basis.  Relying on implied consent for using or sharing personal/confidential patient information for secondary purposes such as these goes beyond the *reasonable expectations* of patients and service users.  Even where a patient or service user has previously given their explicit consent for personal/confidential patient information to be disclosed to a researcher, it would be wrong to assume that they would be content for their information to be disclosed on a second occasion (e.g. a patient who consented to participating in a cancer research study might not give their permission for personal/confidential patient information to be disclosed for research into mental illness; or a service user who consented to personal/confidential patient information being disclosed to a national quality assurance audit might object to the same information being disclosed to a local authority conducting a review into how it organises social care services).

|  |
| --- |
| **Assurance checkpoints**   * A statement, for each of the organisations involved in the collective sharing, setting out;   + purpose   + lawful basis for processing   + duty of confidence satisfied * LHCR will have a Privacy notice stating what data is collected, stored, shared and retained and for how long. The Privacy Notice must also include information on patient preferences * Agreed approach across each LHCR to deal with patients who object to the sharing of their data for to support their individual care * Evidence of effective Role Based Access Control (RBAC) * Evidence of completed DPIA for each data sharing purpose |

### 4.2.5 The Duty of Transparency

The duty of transparency is one of the ways we can build trust and gain the respect of the public in the use of their data. A new requirement of the GDPR is the principle of *accountability* which requires that organisations must be able to demonstrate compliance. Part of this involves transparency and the provision of information to the public – previously referred to as fair processing.

A specific requirement of the GDPR is that organisations must include their lawful basis for processing in information provided to patients, service users and staff, as well as informing individuals of their right to object to processing and how to exercise that right (see 4.7, 4.8).

Whilst we do not need to ask permission to use data for individual care, we are under a duty to inform people about **what** we are doing, as well as **why** and **how** we are doing it. (GDPR Articles 13 and 14).

The law gives discretion to controllers to consider where the information they are required to tell people is displayed and which different layers of communication to adopt.

It is however clear that information regarding the processing of personal data must be:

* Easily accessible (paper or electronic if requested or directed to the website)
* Concise, transparent and intelligible
* Written in clear, plain language
* Free of charge

Care must be taken if conveying information to children as more specific obligations will apply[[6]](#footnote-7). There are also differences in what you must provide depending upon whether you are collecting information directly from individuals or whether it is being obtained from a third party.

It is helpful, if possible, to involve communications professionals in this process. It is important to ensure that the production of materials, language used and channels used are appropriate.

Individuals have the right to know who has access rights and has accessed their record for processing based on Role Based Access Control (RBAC); hence organisations should consider how they would manage these requests.

Where patient information is accessed, only relevant information should be seen. If it is proposed to allow access to a patient’s entire record (‘whole record access’) then the patient’s explicit consent must be sought.

On-line information can form part of the duty of transparency and can assist in helping to keep the data relevant and accurate. The publication of records of processing activities (RoPA), data sharing flows etc., can all contribute to this aim (consider Freedom of Information Act 2000).

To ensure a consistency throughout the LHCR it is important that the same messages and language are used and when new organisations join the LHCR, transparency information will need to be updated.

Equally, to ensure consistency across the system, template text for national initiatives such as the national data opt-out template or local requirements such as DPIA and privacy notices must be adopted. Further guidance on transparency can be found in Appendix H (4.2).

For tools and templates to support this section please see Appendix H (4.2).

|  |
| --- |
| **Assurance Checkpoints**   * Privacy notice(s) stating what data is collected, stored, shared and retained (for how long). The Privacy Notice must also include information on patient preferences * Production of a clear plan, list of communication materials and channels * Copies of the information provided to the public/patients * Evidence of publication of transparency materials by all organisations in the LHCR * Details of a process for monitoring and updating communications * Evidence of publication of information to the public such as Records of Processing, sharing agreements. * Adoption of online access capability and ability to demonstrate uptake (if available) * Evidence of public engagement to gain their view of the approach and test materials |

## 4.3 Determining data flows and controllership

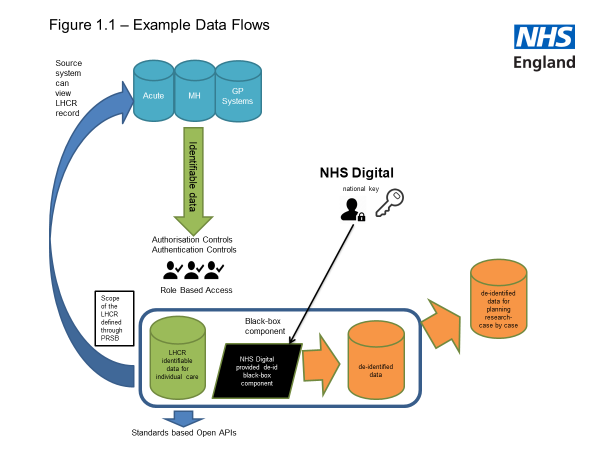
One of the most important challenges in the planning stages is to identify the flow/s of the data, and at each point in the process determine who the controller/s and or processor/s are. This demonstrates a clear pathway to enable better risk identification and mitigation and clarity of who will have responsibility and accountability at each stage. This is particularly important when multiple joint controllers are required such as in a LHCR. A data flow mapping exercise will also inform your Data Protection Impact Assessment (DPIA) and will assist you in accessing data from other organisations such as NHS Digital. (For guidance on controllership and flows see Appendix H (4.3).

Nationally we have worked closely with LHCR Exemplar localities to learn lessons from existing architectural approaches and, whilst LHCRs are operating to a common architectural model, this is being implemented in different ways. As a result of differences in how data is captured at the point of care, differences in digital maturity and local coding, there is the need to be able to bring data together locally from organisations to process, standardise coding and handle duplicate entries. At this stage, we believe that the creation of an abstracted data layer is the safest mechanism to ensure data is available in a normalised and standardised format, but over time we expect to move to an API-based model where data remains resident within its host system.

The objective is to provide a consolidated and standardised representation of a patient’s record for care professionals involved in the direct care of that patient (including, for example, consolidated medication lists, test results etc.) with confidence that it is timely, complete and accurate. The LHCR approach will also provide a feedback loop back to source systems to support the improvement of data quality at source.

To support front-line care professionals in accessing the pertinent information about an individual, the Professional Records Standards Body (PRSB) are, in consultation with care professional groups, outlining what would be included within an individual’s core record. To assist in decision-making, this core content will be developed into a standardised form e.g. enabling a care professional involved in the treatment and care of a patient to be able view a consolidated medication record, run algorithms to be able to identify gaps in care, proactively notify other care professionals and identify patients as risk.

For secondary uses rather than direct care using a set of defined controls outlined within the Information Governance Framework along with a clear legal basis, personal/confidential patient information will be de-identified using de-identification software procured for national use by NHS Digital and deployed locally. This will allow the LHCR to locally de-identify the longitudinal records in their area.  The longitudinal records are not transferred to NHS Digital as part of this process.  Once the data is de-identified it will be used by the LHCR for a defined set of uses e.g. with planning local services.  Use of the data beyond the LHCR will require a use case and appropriate controls/security in place to ensure that individuals cannot be re-identified.  Any use of personal/confidential patient information will require a legal basis*.* Further information is included in journey 3 and 4 of the IG framework. The following diagram helps show the long term plans for data flows.



### 4.3.1 Joint Controllership

The GDPR/Data Protection Act 2018 removes the concept of controllers in common. There is now a clear distinction between controllers working together as joint controllers or alone as individual controllers. Organisations working as part of a LHCR will work as joint controllers with other members of the LHCR areas, because between them they will decide on the purpose and manner for which personal data is collected; it will not be decided by one single organisation within the LHCR. As a LHCR is not a legal entity, joint controllers will need to enter into binding contracts/processing agreements with data processers as a “group” of data controllers rather than appoint a single lead data controller to act on behalf of the group.

Data protection legislation requires joint controllers to be transparent about their respective responsibilities ensuring that individuals know who to contact when wanting to exercise their information rights under the legislation. Information about the joint arrangements must be made to individuals and, irrespective of the joint arrangement, an individual may exercise their rights in respect of and against each controller. Therefore, good processes need to be in place to manage such situations (See Appendix J – GDPR Article 26 – Joint Controllers).

Presently the way in which the above can be met is by setting out an agreement containing the details of those involved in the joint LHCR data controllership and how it will work (a ‘joint controller agreement’).

A joint controller agreement should be an operating model that documents the legal basis, the roles and responsibilities of each controller in the group. It should detail common rules for things such as retention and disposal and the agreement should specifically explain who will deal with requests from individuals to exercise their rights under the GDPR.

As part of the joint data controllership arrangements, the constituent legal entities need to agree how they will handle access requests, and which includes how decisions will be made on whether or not to redact third party data.

It is important to note that a ‘joint controller agreement’ is not the same as a written contract or other legal act which is required when using a processor (GDPR Article 28), nor is it a legal “service level agreement”. However, it would be sensible that if a LHCR, as a grouping, requires a service level agreement, a ‘joint controller agreement’ and, where they are working with a processor, a written contract that the separate agreements are brought together into a suite of documentation as a single joint operating agreement.

It would also be good practice to make joint controller agreements available to the public through the participating organisations publication schemes. This would help meet the duties of accountability and transparency.

With regards to liability joint controllers can be held “jointly liable” if collectively they are responsible for any breach of data protection law, however the ICO as the regulator will investigate to establish which organisation is at fault before using any enforcement powers, therefore not all controllers (as part of a joint controllership agreement) will be liable all of the time[[7]](#footnote-8).

### 4.3.2 Data sharing arrangements

LHCRs will also share patient information with other health and care organisations that are not part of the LHCR. At times this sharing will be done on an ad-hoc basis but in some situations the sharing will be more regular and possibly at a large scale (for example when an adjacent LHCR area contains specialist treatment centres). The Information Commissioner's Office (ICO’s) Data Sharing Code of Practice remains current under the new data protection legislation. The Code covers how to approach ad-hoc and more regular data sharing and how to record activities using data sharing agreements.

In accordance with the ICO Data Sharing Code of Practice, a data sharing agreement is useful only when the ‘sharing’ is between controller to controller and not between a controller and a processor. When processors are engaged, a written contract or other legal act is always required which may be supplemented by a separate data processing agreement.

Individuals can seek compensation from joint controllers in exactly the same way as from a sole controller. Each joint controller will be liable for the entire damage caused by the processing, unless it can prove it is not in any way responsible for the event giving rise to the damage. The arrangement made between controllers is irrelevant for these purposes.

For tools and templates to support this section please see Appendix H (4.3). This includes a decision tree regarding Data Sharing requirements.

|  |
| --- |
| **Assurance Checkpoints**   * A single agreement that will incorporate various documents as listed below:   + Data Sharing Agreements/Protocols for the grouping   + A written contract between the grouping and the processor/s   + A clear data processing map showing purpose and controller and processor at each stage of data flow.   + Service level agreements   + Standard contract clauses |

## 4.4 Records of Processing Activity Art.30

Data protection legislation requires records of processing activities to be kept. These records must be kept up to date by controllers and processors as they can be requested by the supervisory authority at any time. Records of processing activity can be linked to privacy notices for ease of transparency.

From the records of processing activity, organisations will be able to build upon and manage a comprehensive register of information assets and their owners, showing when, why and how that data is processed for what purposes, with whom it is shared and retention periods. The registers should be monitored, reviewed and maintained on a regular basis.

Where possible the registers should be released through the organisations’ publication schemes. Publication will assist in demonstrating accountability. For tools and templates to support this section please see Appendix H (4.4).

|  |
| --- |
| **Assurance Checkpoints**   * Records of Processing Activity evidence / Production of an Information Asset register * Policies and procedures for information asset management |

## 4.5 Assuring security

All organisations within a LHCR are expected to adhere to current published guidance for health and care to ensure they implement and develop cyber security to protect the confidentiality, integrity and availability of records, and to ensure that people, processes and technology are maintained to underpin cyber security. Organisations are expected to comply with relevant legislation, such as the General Data Protection Regulations 2016, The Network and Information Systems (NIS) Regulations 2018 and relevant policies and guidance (see Appendix K – Security Requirements).

**NB:** A LHCR Cyber Security Framework is under development and anticipated to be published prior to release of the final Information Governance Framework.

One way of showing compliance with this obligation is by meeting the requirements of the data security and protection toolkit (DSPT)[[8]](#footnote-9), however this is not the only way to demonstrate compliance.

It is also important those policies for areas such as; staff training, internal audits and HR policies, retention and disposal schedules are not only published, but can be shown to have been adhered to.

Any use of a processor should be aligned to legal and contractual obligations.

### 4.5.1 Using Processors

A processor should only be engaged if the controllers have been provided with sufficient guarantees that the appropriate technical and organisational measures have been implemented in such a way as to meet the obligations of data protection law (specifically Articles 28, 29, 30 and 32 of the GDPR) and will ensure the protection of the rights of the data subjects.

All GP Practices will use a clinical system of their choice, usually procured by the CCG on behalf of its member practices. As part of this, the system supplier provides a *Deed of Undertaking* which indemnifies GPs. This Undertaking sets out what controls will be in place if the system supplier processes data itself and/or uses a sub-processor and provides assurances to GPs that compliance will be adhered to in relation to data protection law[[9]](#footnote-10).

If using a processor, a written contract must be in place between the group of organisations acting as joint controllers and the processor/s. This is a legal requirement and is essential so that everyone understands their roles and responsibilities and assurance can be given that the processor operates in a legally compliant way.

Processors may only act under written instruction from a controller, they must gain authorisation from the controller/s if they wish to sub-contract to a third party. They must also ensure the security of their processing, keep records of their processing and notify the controllers of any breaches which occur, without undue delay. When working as a group of joint controllers it is important to decide if the processor will be instructed by a lead organisation or by all of them.

Processors also required to have a DPO therefore the LHCR Information Governance Lead should take responsibility for liaising with the DPO in the data processing organisation to ensure clarity and compliance.

Technical specifications such as role-based access, overrides etc. should be carefully considered and all the controllers comfortable with the arrangements.

### 4.5.2 The Data Security and Protection Toolkit (DSPT)

All organisations processing NHS patient data must meet the requirements of the Data Security and Protection Toolkit (DSPT), The DSPT is a compliance framework that covers all aspects of security and confidentiality linked with and supported by National Cyber Security Centre, the agency tasked with protecting critical infrastructure.

The focus of the DSPT is on building trust in health and care IT systems based on the National Data Guardian’s ten data security standards. The DSPT is structured to require organisations to comply with relevant information governance standards. These are for each of the ten standards. To meet the relevant Standard all Toolkit questions must be appropriately answered. Organisations must not rely solely on DSPT returns for assurance.

The DSPT also includes a tool for reporting data breach incidents which must be used by NHS-funded care organisations. (See Appendix O for more information on Data Breach Management)

Any use of a processor should be aligned to legal and contractual obligations. Suppliers of software and services to care organisations are also required to complete the DSPT.

For tools and templates to support this section please see Appendix H (4.5).

### 4.5.3 Data and Cyber Security Standards

LHCRs must be able to demonstrate the security of the confidential patient information within their platform at rest and in transit. This is not limited to the successful completion and audit of the DSPT as there are other activities that the LHCRS need to undertake:

* LHCRs will comply with the National Data Guardian’s 10 Data Security standards[[10]](#footnote-11). These standards apply to every organization handling health and social care information although the way the standards apply will vary according to the size and type of organisation.
* LHCRs will assure themselves of the security status of systems wishing to connect in-line with guidance developed in conjunction with NHS Digital and the National Cyber Security Centre (NCSC).
* LHCRs will undertake independent onsite assessments and work with the programme, NHS Digital and NCSC to achieve an appropriate level of cyber security in line with industry best practice.

For tools and templates to support this section please see Appendix H (4.5).

4.5.4 Effective Cyber Threat Situational Awareness

Organisations need to have effective cyber threat situational awareness so that they can respond in a timely, effective and safe manner to cyber threats and risk to their data and technology. Care Computer Emergency Response Team (CareCERT) is established by NHS Digital to provide threat intelligence, advice and guidance to support health and social care organisations in this task.

Organisations on the N3/TN/ HSCN network can access the CareCERT Information Sharing Portal which provides threat intelligence and information security alerts. Organisations that are not on the N3/TN/HSCN network (such as some Social Care Providers) will not be able to access CareCERT Information Sharing Portal however, these organisations can sign up to receive a weekly bulletin of threat intelligence articles taken from the Portal by sending an email to carecert@nhsdigital.nhs.uk (organisations that ‘are’ on N3 should also do this anyway unless they plan to check the portal every week).

|  |
| --- |
| **Assurance Checkpoints**   * Publication and evidence of compliance with policies for areas such as staff training, internal audit, HR policies, retention and disposal schedules. * Evidence of annual completed and (where there is a mandatory requirement) audited Data Security and Protection Toolkit to meet the mandated requirements for example   + - Records of processing activities are documented     - Cyber assurance * Evidence of independent onsite assessments * Board approved action plan if mandated requirements not met * Evidence of organisations signed up to receive cyber threat intelligence from CareCERT |

## 4.6 Data Access, Review and Retention

When accessing data for individual care purposes, consideration must be given to the policies and processes used to support that disclosure.

Following the data protection principles when using personal data, the amount of data should be adequate for the purpose and not excessive.

Who has access and what they have access to needs to be worked out and made clear within the information sharing agreements and information provided to the public. An appropriate access control model delivers this commitment.

Patients have the right to know who has access rights and has accessed their record for processing. They also have the right to challenge that access. This is a fundamental principle and essential for maintaining public trust.

LHCRs need to ensure that only health and care professionals who have a **legitimate relationship** with the patient, in the delivery of their care, will have access to their patient record. This will ensure that the level of access to confidential patient information is “necessary and proportionate”.

LHCR’s must include high-level audit functionality which enables controllers to meet their access control responsibilities as well as being able to provide information to patients about who has accessed their records, when and why.

LHCR’s must ensure that they retain records in an accessible format until the relevant retention period is reached, in line with the Records Management Code of Practice 2016. A decision must then be made as to whether the record should be:

* retained for a longer period (there must be a valid reason for this)
* sent to a Place of Deposit
* destroyed / deleted.

For tools and templates to support this section please see Appendix H (4.6) and Appendix P.

|  |
| --- |
| **Assurance Checkpoint**   * Data Maps * Data Processing Contract * Evidence of approved and completed Data Protection Impact Assessment (DPIA) for each data sharing purpose * Data Sharing Agreement (DSA) * Evidence of compliance with the Records Management Code of Practice for Health and Social Care 2016 * Policies and audit * Evidence of effective Role Based Access Control (RBAC) |

## 4.7 Individual Rights

The GDPR offers individuals clear rights in certain circumstances; those rights are:

* Right to be informed
* Right of access by the data subject
* Right to rectification
* Right to erasure (Right to be forgotten)
* Right to restriction of processing
* Right to object to processing
* Right to data portability
* Rights in relation to automated decision making and profiling

All organisations must have policies and procedures in place ensure the appropriate management of individual rights. For more detail on Individual Rights and restrictions under GDPR see Appendix N.

Care should be taken to ensure that the LHCR is clear on which individual rights apply and have processes in place to ensure an individual can enact those rights.

The application of individual rights is dependent upon the conditions for processing used for the sharing of the data.

In all circumstances the individual has a right to obtain confirmation as to whether personal data is held about them and to have access to that data and the associated information namely;

* the purposes of the processing
* the categories of the data
* recipients of the data and who has accessed it
* how long the data will be stored and the criteria used to determine that
* the existence of the right to request rectification or erasure, restriction and objection to processing should those rights be applicable

There needs to be a process in place to ensure that Subject Access Requests to the LHCR are responded to.  This should be detailed in the joint controller arrangement.  An example of a process which has worked well in some areas is an information sharing group is established which leads on the request.  In the event of a Subject Access Request, each organisation contributing to the LHCR would be asked to send their redacted data to the information sharing group who would respond to the individual. It must be made clear to individuals that this is the process in case some individuals do not want information sent outside the organisation that holds it. It such cases the ‘holding’ organisation should deal with the request on an exclusive basis.

Fees can no longer be charged for subject access except in instances where the request is manifestly excessive or unfounded, particularly if it is repetitive. In these instances, organisations may charge a reasonable fee but this must only be based on admin costs involved in retrieving information.

For tools and templates to support this section please see Appendix H (4.7).

|  |
| --- |
| **Assurance Checkpoint**   * Process in place for complying with individual rights where required i.e rectification, objection and subject access requests * Demonstration of how to exercise individual rights in transparency documentation * Evidence of agreed approach to managing patient objections to share their data for individual care under the LHCR |

## 4.8 Patient Objection to Processing and National Data Opt-Out

### 4.8.1 National data opt-out

The national data opt-out is a service that allows people to opt out of their confidential patient information being used for research and planning and therefore does not apply to data used for individual care purposes (for definition see Appendix D). It is available at [www.nhs.uk/your-nhs-data-matters](http://www.nhs.uk/your-nhs-data-matters).

The national data opt-out programme has set out clear operational policy which must be applied by LHCRs.

* The national data opt-out:
  + Does not apply to individual care.
  + Does not apply to data which is anonymised in accordance with the ICO’s code (currently under revision to meet GDPR requirements).
  + Does not apply where there is explicit consent.
  + Does not apply where there is a legal requirement for the information.
  + Does apply to approvals made by the Confidentiality Advisory Group (CAG) under the NHS Act 2006 section 251.

As the current intention in LHCRs, for purposes other than individual care, is to use data which is anonymised in accordance with the ICO’s code – the national data opt-out would not apply. However, if a LHCR decided to share confidential patient information, with section 251 support, the national data opt-out would need to be applied. The national data opt-out also needs to be applied if an organisation shares confidential patient information outside of the LHCR for research and planning e.g. a Trust which is part of the LHCR is involved separately in a research project. All health and care organisations will be expected to comply with the national data opt-out by March 2020.

LHCRs will bring a range of benefits and will play an important role in making patients aware of these benefits.  Local resources can support patients in making their choice by explaining the local benefits e.g. by providing patients with local evidence, case studies or stories of how sharing improves care.

It is still important though that the LHCR organisations include information about the national data opt-out in their transparency materials.

Further information about the national data opt-out including detailed operational policy guidance and guidance on compliance is available at: <https://digital.nhs.uk/services/national-data-opt-out-programme>.

### 4.8.2 Patient Objection to Processing

Article 21 of GDPR gives individuals the right to object to the processing of their personal data and have their objection considered. The right to object is particularly relevant to certain health and care organisations where lawful processing is based on the ‘public interest’ provision. If someone objects to you processing his or her data, you will need to demonstrate ‘compelling, legitimate grounds for [either] the processing which overrides the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims’.

Organisations need to ensure that where objections have been received, procedures and processes are in place to consider and respond where an individual objects. Patient objections under Article 21 must be considered on a case-by-case basis. An individual must give specific reasons why they are objecting to the processing of their data based on their particular situation. A patient must have the risks of their decision clearly explained to them and documented. When considering whether to uphold an objection, the compelling grounds need to be balanced by the individual's original grounds for the objection, which will differ from case by case. Controllers will then need to consider whether their own requirements override that of the individual.

All LHCRs must ensure procedures are in place in relation to patient objections under GDPR as a minimum. Some LHCRs may go beyond this, following local discussions with health and care professionals and patients and implement a local policy where a patient is asked before their record is viewed (this should not be referred to as ‘patient consent’). This may be in the short term and over time it may become routine and expected for the record to be accessed by those caring for a patient and clinicians and patients may decide this additional step is not needed.

Although GDPR does not give a specific definition of compelling legitimate grounds there is guidance from the ICO on legitimate interests for processing data which includes a Legitimate Interest Assessment (LIA). The LIA encourages a data controller to ask the right questions about processing and objectively consider what the reasonable expectations of the individual is and any impact of the processing on them via a three part test. The Balancing Test (part 3 of the LIA) covers the need to consider the interests and fundamental rights and freedoms of the individual. The guidance can help aid decision making on whether an organisation could continue to process the data subject’s data on compelling and legitimate grounds. The guidance looks at the nature of the data, reasonable expectations, the potential impact on the individual and any damage that the processing might cause.

Some LHCR areas have also provided mechanisms for patients to state a preference over whether they have a shared record e.g. by providing an opt-out form. Again this is a local policy decision (See Appendix Q for some template text for LHCRs to utilise). It is important however that this is not confused with the right to object under GDPR where each objection needs to be considered and responded to on a case-by-case basis. Communications with patients should be clear and distinguish between the right to object under GDPR and a patient preference around data sharing.

For tools and templates to support this section please see Appendix H (4.8).

## 4.9 Demonstrating Accountability

The GDPR requires all controllers to demonstrate their compliance with the Regulation (Article 5 (2) which relates to accountability.

The UK regulator, the ICO, has set out that organisations can demonstrate their compliance as outlined below. It is therefore imperative that all decision making is documented, who was involved and the rationale/justification behind the decision

### 4.9.1 Adopting principles by design and default

Adopting the principles of data protection by design and data protection by default is an important concept in regard to any project or new model of care. It is important that the consideration of new ways of working consider the impacts to privacy and confidentiality at the design stage. That way information governance is integrated into the policies, processes and systems from the beginning. It will assist in enabling data sharing for the benefit of individuals and the system, whilst minimising the risk to privacy. Information governance should be identified as part of any Project Initiation Documents and should be treated in the same way as finance. assessing the essential criteria, key issues, resources etc.

A data minimisation approach should be adopted. Only where there is no alternative to its use should personal data be used for any purpose. Personal data will always be required for the purpose of individual care; however, caution should be taken to ensure that a balance is sought between the requirement for adequate amounts of data for the provision of care versus the processing of excessive information (taking into account any clinical risk). Clinical Safety Officers (CSO) as well as Caldicott Guardians and Data Protection Officers must be involved with such decision making.

### 4.9.2 Data Protection Impact Assessments (DPIA)

If personal data is to be used GDPR r.84 states a DPIA is required “*where processing operations are likely to result in a* ***high*** *risk to the rights and freedoms of natural persons*”. Article 35 further sets out that one of the situations where a DPIA is required is where the processing will involve large amounts of ‘special category data’ data’. Any decision not to carry out a DPIA must be justified and documented.

You must have a mechanism for ensuring DPIAs are appropriately undertaken and acted on. This includes training for staff so they understand the need to complete a DPIA, along with the policies and processes they need to follow.

When completing the DPIA if you identify a high risk which you cannot mitigate then you MUST consult the ICO before starting the processing.

For tools and templates to support this section please see Appendix H (4.9).

|  |
| --- |
| **Assurance Checkpoint**   * Completed and approved DPIA for each data sharing purpose * Evidence of information governance considerations in Project Initiation Documentation * Evidence of DPIA risks incorporated into (organisational/LHCR) risk register including mitigation and management * Evidence of consultation with the public on the DPIA * Evidence that unmitigated high risks are escalated to the DPO and the ICO is consulted |

# Journey 1 – Individual care within a LHCR (between health and social care bodies)

**Introduction**

For individual care purposes, service providers can receive and share personal/confidential patient information by ensuring that they meet the lawful processing conditions as controllers.

When sharing you need to be very clear about the purpose for which the information is being used. If it does not fit into the definition set out in Appendix D it will not be considered as individual care and therefore the way in which the information governance rules apply will change (See journeys 3 and 4).

Appendix D provides a definition of direct/individual care as defined in Dame Fiona Caldicott’s Information Governance Review 2013. In line with the advice of the Understanding Patient Data project this document has substituted the term “individual care”. Its meaning and the conditions attached to it are exactly the same as the definition of direct care in Dame Fiona’s 2013 review.

See Appendix C for a detailed governance process.

**Example Tasklist (not exhaustive)**

By completing this tasklist, this will help GDPR Art. 30 requirements for ROPA.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Task** | **Tools and Template/Appendix** | **Complete** |
| 1 | Describe your care system’s structure | Appendix H (4.1) |  |
| 2 | Define how your care system will govern data use | Appendix C  Appendix H (2.1) |  |
| 3 | Identify the lawful basis for your data sharing activities and allocate them | Appendix H (4.2) |  |
| 4 | Understand what data you require | Tbc – data mapping |  |
| 5 | Demonstrate how you will protect the data | Appendix H (4.5) |  |
| 6 | Ensure appropriate contracts and agreements are in place | Appendix H (4.3) |  |
| 7 | Assure your population that processing is fair and transparent | Appendix H (4.2) |  |

# Journey 2 – Individual Care Across Geographical LHCR Boundaries

**Introduction**

Where relationships already exist with neighbouring LHCRs, i.e. known shared clinics, established patient flows, etc, then information sharing arrangements should be developed similar to intra LHCR sharing (journey 1).

There may also be circumstances for ad hoc information sharing. In such circumstances, professional judgement needs to be exercised and an awareness of professional guidance or ethical rules that are likely to be relevant to the type of decisions about information sharing across care settings. The ICO data sharing code of practice[[11]](#footnote-12) provides information for such circumstances.

It is important that information is available at the point of care for a patient. A requirement of LHCRs is that there is the ability to share information with other LHCRs through common and open interfaces subject to agreed access control arrangements, including the logging of all such accesses. Having a common standard core of information regardless of the means of implementation will be fundamental to ensure that a LHCR record is safely and securely transferable between LHCRs, as and when patients move between them. The Professional Records Standard Body is developing this core record through engagement with health and care professions and patient.

In terms of the information governance, Journey 2 of the IG framework covers individual care across geographical LHCR boundaries. Where relationships exist with neighbouring LHCRs i.e. known shared clinics, established data flows etc. then information sharing arrangements should be developed similar to intra LHCR sharing. Information will be added in due course to provide further about sharing the LHCR core record between LHCR areas.

**Discovery of data about a patient**

Where a person receives care at a venue outside of their home LHCR there is a need to discover where data is held so the data can be retrieved. The intent is for the following capabilities to support the discovery of the location of data for Journey 2:

* PDS - to hold LHCR of Record and provide an API that returns both a person’s NHS Number and LHCR of Record
* NRLS – to hold pointers to data published by non-LHCR areas and pointers published by LHCRs
* LHCR APIs – to enable retrieval of data subject to authentication and authorisation

**Example Tasklist (not exhaustive)**

By completing this tasklist, this will help GDPR Art. 30 requirements for ROPA.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Task** | **Tools and Template/Appendix** | **Complete** |
| 1 | Describe your care system’s structure | Appendix H (4.1) |  |
| 2 | Define how your care system will govern data use | Appendix C  Appendix H (2.1) |  |
| 3 | Identify the lawful basis for your data sharing activities and allocate them | Appendix H (4.2) |  |
| 4 | Understand what data you require | Tbc – data mapping |  |
| 5 | Demonstrate how you will protect the data | Appendix H (4.5) |  |
| 6 | Ensure appropriate contracts and agreements are in place | Appendix H (4.3) |  |
| 7 | Assure your population that processing is fair and transparent | Appendix H (4.2) |  |

DN – national RBAC model to be developed

# Journey 3 – Improving health, care and services through planning and evaluation (Secondary Uses/Population Health Management)

**Background**

This journey covers the use of data for improving health, care and servicing through planning/ health service management. Using information beyond individual care results in different information governance requirements and implications for access to data to support them. Data from LHCRs will be used for the provision of health and care, for planning and evaluating services and for the promotion of health. It will not be used for example for marketing or insurance purposes.

The appropriate lawful basis for processing personal data under the DPA(GDPR) is set out below. Personal/confidential patient information will be de-identified using de-identification software procured for national use by NHS Digital and deployed locally. This will allow the LHCR to locally de-identify the longitudinal records in their area.

Further information will be added to the Information Governance Framework, which will set out the controls and security which will need to be in place to ensure that patients cannot be re-identified from the data and it is therefore considered anonymous and out of scope for some of the GDPR requirements. Any use of personal/confidential patient information will require a legal basis as follows*.*

**Lawful Basis for Processing Health and Care Records**

6 1 (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The Health and Social Care (Safety and Quality) Act 2015 inserted a legal Duty to Share Information In Part 9 of the Health and Social Care Act 2012 (health and adult social care services: information).

|  |  |
| --- | --- |
| Local Authorities | Care Act 2014 (Section 6)  Local Government Act 1974  Local Government Act 1972 (Section 111)  Localism Act 2011  Localism Act 2000 (Section 1)  Children Act 2004  Children Act 1989 |

If the data processed for the purposes of service planning and managementit is still considered to be personal data under GDPR. The condition which supports the processing of special category of data is:

9 (2) (h) - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

**Secondary Uses Data Governance Tool (SUDGT)**

In order for LHCR data to be used for secondary uses, the joint controllers responsible for the LHCR must agree and implement a robust method to ensure the data is de-identified sufficiently to render it anonymous in line with the ICO Anonymisation code of practice.[[12]](#footnote-13) The SUDGT proposes different models to achieve this and sets out the pros/cons associated with those models. The tool also includes contractual processing models dependent on the purpose for the use of the data and the statutory duties of the organisations involved

For individual care activities, service providers can receive and share personal/confidential patient information by ensuring that they meet the lawful processing conditions as controllers. Where there is a requirement to use data for purposes beyond individual care (secondary uses/Population Health Management [PHM]), organisations need to ensure they have the legal basis to undertake the activities, including processing to remove patient identifiers.

In many instances, patient level anonymous data is required by commissioners in order that they can meet their statutory duties and this will provide the legal basis for their access to patient level anonymous data. Where a commissioner contracts another organisation such as a provider to undertake secondary use activities on their behalf, the provider must operate under processing contracts and will only be able to use the data for the agreed purpose. If the 3rd party organisation breaches the conditions and if personal data is involved, this would be reported to the ICO and appropriate action taken. This would be clearly documented in an agreement which would set out the scope of decision making and controls on data processing.

DN – Include reference to the confidentiality requirements in above para (1.13.1.9)

The SUDGT has been developed by NHS England to support Sustainable Transformation Partnerships/Integrated Care Systems (STPs/ICSs) to implement robust governance processes to support their use of data, focused on data required for secondary purposes (see Appendix H (2.1)).

The SUDGT includes a matrices document which lists the statutory duty/lawful basis for processing of each organisation type, mapped to the type of activities which need to be undertaken to meet them. It also maps these to the type of data which may be required. It also proposes contractual and data processing models to enable delegation of secondary purpose activities to providers. Use of the SUDGT considers and builds upon the legal and governance considerations required for compliance and assurance with data protection and privacy. The tool takes the user/s through 6 steps as shown on the slide below:



**Example**

Consider any additional requirements for sharing de-identified data across, within and outside geographical boundaries to improve the service and outcomes (secondary uses).

NHS England have developed a web version of the SUDGT. The first iteration of the tool was made available at the beginning of January 2019. NHS England are working with South Central and West CSU who are training information governance and BI (Business Intelligence) Leads within each NHS England CSU to ensure they can support STP/ICS to use the tool and subsequently set up their governance boards appropriately. Use of the SUDGT will also ensure that appropriate infrastructure models for the de-identification of data are considered, as well as development of robust Data Protection Impact Assessments, contracts, data processing agreements etc. are completed.

A list of each information governance/BI Lead associated with STPs/ICSs is included in the web version of the tool and will be included in this framework in due course.

A list of each information governance/BI Lead associated with STPs/ICSs is included in the web version of the tool and will be included in this framework in due course.

**Example Tasklist (not exhaustive)**

By completing this tasklist, this will help GDPR Art. 30 requirements for ROPA.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Task** | **Tools and Template/Appendix** | **Complete** |
| 1 | Describe your care system’s structure | Appendix H (4.1) |  |
| 2 | Define how your care system will govern data use | Appendix C  Appendix H (2.1) |  |
| 3 | Identify the lawful basis for your data sharing activities and allocate them | Appendix H (4.2) |  |
| 4 | Understand what data you require | Tbc – data mapping |  |
| 5 | Demonstrate how you will protect the data | Appendix H (4.5) |  |
| 6 | Ensure appropriate contracts and agreements are in place | Appendix H (4.3) |  |
| 7 | Assure your population that processing is fair and transparent | Appendix H (4.2) |  |

# 8. Journey 4 – Research

**Introduction**

This part of the framework sets out the issues that need to be considered before using patient information for medical research purposes.

The Health Research Authority (HRA) have set out a UK Policy Framework for Health and Social Care Research:

<https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/uk-policy-framework-health-social-care-research/>.

Understanding the role of the HRA and its approvals process will be the key to undertaking successful (and legal) medical research. If you plan to conduct any form of research you will require it to be approved by the HRA. They provide a decision tool to help organisations to determine if a project is research:

<https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/>.

Once you are clear that your project is medical research you will need to consider what needs to be done to meet information governance requirements. This will depend on a number of factors including whether the information is personal/confidential patient information and/or special category data and the controls in place.

**Anonymous data**

Anonymous data is not subject to the common law duty of confidence or data protection laws because individuals cannot be identified. However, because the source of such information will be information about a specific patient’s condition then it will be patient information, as defined under the NHS Act 2006 – see footnote below.

**Personal/Confidential Patient Information**

To use this kind of information/data requires high information governance standards (and which apply to data that has been pseudonymised) to be met. If an individual can be re-identified either accidentally or deliberately then this information should be treated as confidential patient information/personal data. How to go about using this type of information/data is set out in the section below.

**Data Protection**

Under the GDPR/Data Protection Act 2018 personal data about an individual’s health is classed as ‘special category’ personal data. Further requirements are set out under the law that must be met before this type of data can be used.

The HRA has provided guidance for researchers and study co-ordinators:

<https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/>.

They have also produced material for data protection officers and research governance managers:

<https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/>.

**Confidential Patient Information (CPI)**

The next consideration is how to meet the requirements of the common law duty of confidence (CLDC) and which applies to ‘confidential patient information’ as defined under the NHS Act 2006.

The HRA is responsible for the operation of the Confidentiality Advisory Group (CAG)[[13]](#footnote-14) which considers applications for support under the NHS Act 2006 s251. This allows the HRA to set aside the duty of confidence where confidential information is required for medical research and obtaining patient consent is not feasible.

If the planned medical research is based on gaining the explicit consent of patients then this will satisfy the requirements of the CLDC (note an alternative condition to explicit consent should be used to satisfy data protection compliance). However, where it is planned to use confidential patient information for medical research without the explicit consent of patients because it is not feasible, then an application will need to be made to CAG through the HRA approval’s process. The details on how to make such an application can be found here:

<https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/confidentiality-advisory-group/>

**Medical research ethics**

Although technically part of an organisation’s Caldicott Guardian role, there does need to be information governance awareness of the requirement for ethical approval from a Research Ethics Committee (REC) which are also run by the HRA. The reason for this is that without REC support, any processing of data for health research would not be being undertaken with a lawful basis even if the explicit consent of patients was obtained. This in turn breaches the requirement of Art. 5 (1)(a) of the GDPR.

**Digital Innovation Hubs**

Health Data Research UK is leading on the delivery of Digital Innovation Hubs which will support the responsible and safe use of data for research and innovation.  The Digital Innovation Hub Programme aims to enable a UK-wide life sciences ecosystem that provides access to health data, technology and science, research and innovation services to ask and answer important health and care questions.   Anonymous data from LHCRs could in the future contribute to answering some of these questions.  Digital Innovation Hubs will not change the legal basis for accessing data so the information governance requirements set out in this journey will apply.  Any use of confidential patient information would require patient consent or section 251 support.

# Appendices

## Appendix A - Glossary for the Information Governance Framework

**Glossary**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Accountability | Accountability is one of the data protection principles - it makes the Data Controller responsible for complying with the GDPR and able to demonstrate compliance. |
| Anonymous Data | Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. |
| Biometric data | Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (finger print) data. |
| Breach | Any failure to meet the requirements of the Data Protection Act and/or GDPR, unlawful disclosure or misuse of personal data and an inappropriate invasion of people’s privacy. |
| Caldicott Guardian | A senior person in an organisation responsible for protecting the confidentiality of patient information and enabling appropriate information sharing by providing advice to professionals and staff. |
| Clinical Commissioning Group (CCG) | Groups of GP practices, working with other healthcare professionals, which are responsible for commissioning most health and care services for patients. |
| Clinical Safety Officers (CSOs) | Person in a Manufacturer’s organisation responsible for ensuring the safety of a Health IT System in that organisation through the application of clinical risk management.  Further information about the responsibilities of a Clinical Safety Officer is set out in the clinical safety standards. <https://digital.nhs.uk/services/solution-assurance/the-clinical-safety-team> |
| Commissioning | Commissioning is essentially buying care in line with available resources to ensure that services meet the needs of the population. The process of commissioning includes assessing the needs of the population, selecting service providers and ensuring that these services are safe, effective, people-centred and of high quality. Commissioners are responsible for commissioning services. |
| Commissioning Support Unit (CSU) | Clinical Commissioning Support Units provide Clinical Commissioning Groups with external support, specialist skills and knowledge to support them in their role as commissioners. |
| Common law | Laws that are based on court or tribunal decisions which govern future decisions on similar cases |
| Common law duty of confidentiality (CLDC) | Under the common law duty of confidentiality, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without patient consent. |
| Confidential Patient Information | Defined in section 251 of the National Health Service Act 2006, confidential patient information is information that meets the following three requirements:  1. Identifiable, or likely identifiable (e.g. from other data in possession of the recipient),  2. Given in circumstances where the individual is owed a duty of confidence; and  3. Conveys some information about the physical or mental health or condition of an individual |
| Consent | Consent means offering individuals real choice and control. It requires a positive opt-in and must be evidential. The GDPR sets a high standard for consent. Often consent is not required under GPDR and another lawful basis can be found however consent may still be required under common law. |
| Controller | The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data |
| Cyber threat | The possibility of a malicious attempt to damage or disrupt a computer network or system |
| Data breach notification | A duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The supervisory authority in the UK is the Information Commissioner's Office. |
| Data Protection Act 2018 (DPA) | The Data Protection Act 2018 is the UK’s implementation of the General Data Protection Regulation (GDPR). It transposes the Law enforcement directive into UK law. |
| Data Protection Impact Assessment (DPIA) | A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. Under GPDR a DPIA is required for processing that is likely to result in a high risk to individuals. |
| Data Protection Officer (DPO) | An independent expert in data protection who helps monitor internal compliance, informs and advises on data obligations including Data Protection Impact Assessments and acts as a point of contact for data subjects and the Information Commissioner's Office. |
| Data Security | Protecting data and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. |
| Data Sharing Agreement | A data sharing agreement sets out a common set of rules to be adopted by the various organisations involved in a data sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis. |
| Data Subject | An identified or identifiable natural person. |
| Duty of confidentiality | This ariseswhen one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It –   1. is a legal obligation that is derived from [common law](https://www.connectedhealthcities.org/community/glossary-data-use/#commonlaw); 2. is a requirement established either within professional codes of conduct and/or that must be included within relevant employment contracts. It is also linked to disciplinary procedures through both these requirements.   It would also apply where confidential patient information is received or obtained from another organisation as the data subject would have a reasonable expectation that any recipient would hold it in confidence. |
| Duty of Transparency | The GDPR principle of ‘accountability’ requires that organisations must be able to demonstrate compliance. Part of this involves transparency and the provision of information to subjects – previously referred to as fair processing.  A specific requirement of the GDPR is that organisations must include their lawful basis for processing information provided to patients, service users and staff |
| Explicit consent | Explicit consent requires a very clear and specific statement of consent. It is unmistakeable. It can be given in writing or verbally, or conveyed through another form of communication such as signing. GPDR gives a specific right to withdraw consent. |
| General Data Protection Regulation (GDPR) | The European Union regulation that came into force across 28 EU Member States, including the United Kingdom in May 2018. It forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 |
| Genetic data | Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. |
| Human Rights Act 1998 | The Human Rights Act 1998 sets out the fundamental rights and freedoms that everyone in the UK is entitled to. It incorporates the rights set out in the European Convention on Human Rights (ECHR) into domestic British law. |
| Implied consent | Applicable only within the context of individual care of individuals. Under the common law of confidentiality consent may be explicit or implied. Implied consent refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed.  Examples of the use of implied consent include doctors and nurses sharing personal confidential data during handovers without asking for the patient’s consent. Alternatively, a physiotherapist may access the record of a patient who has already accepted a referral before a face-to-face consultation on the basis of implied consent |
| Individual care | Has the same meaning as *Direct Care defined by the 2013 Information Governance Review:*  *A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals’ ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.* |
| Information asset register | A register of what information you hold. It is a way of helping understand any risks so that an organisation can protect the information. |
| Information Commissioner's Office (ICO) | The UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. |
| Information Governance (IG) | The term used to describe how organisations and individuals manage and handle data within the health and social care system in England. In practical terms, Information Governance is about managing and sharing information appropriately. There is a body of legislation that protects personal information and any information shared inappropriately could mean a fine for the organisation or even prison for an individual. |
| Joint controllers/Joint Data Controllership | Where two or more controllers jointly determine the purposes and means of processing. Joint controllers are not required to have a contract, but must have a transparent arrangement that sets out agreed roles and responsibilities for complying with the GDPR. |
| Joint controller agreement | Joint controllers are not required to have a contract, but must have a transparent arrangement that sets out your agreed roles and responsibilities for complying with the GDPR. |
| Lawful basis | The principle of accountability requires you to be able to demonstrate that you are complying with the GDPR, and have appropriate policies and processes. This **means** that you need to be able to show that you have properly considered which **lawful basis** applies to each processing purpose and can justify your decision |
| Legal entity | A lawful or legally standing association corporation, partnership, proprietorship, trust or individual which has legal capacity to (1) enter into agreements or contracts (2) assume obligations (3) incur and pay debts (4) sue and be sued in its own right, and (5) to be accountable for illegal activities. |
| Legal obligation | The obligation or duty that is enforced by a court of law. |
| Legal vires | Legal powers set out in statute. |
| Local Health and Care Record (LHCR) | Local Health and Care Records will ensure information is collected and made available across local populations to support joined up and safer care. |
| Medical Research | Medical research studies are designed to provide information on health or disease. Organisations processing data for research purposes must have appropriate organisational and technical measures in place. This includes approval from a research ethics committee (as defined in the Data Protection Act) if it involves processing data in order to do or decide something with respect to an individual person. |
| National Data Guardian (NDG) | The National Data Guardian (NDG) advises and challenges the health and care system to help ensure that citizens’ confidential information is safeguarded securely and used properly. |
| National data opt-out | A new service that allows people to opt out of their confidential patient information being used for research and planning. |
| Natural person | A living human being with certain rights and responsibilities under law. |
| NHS Digital Data Security and Protection toolkit (DSPT) | The data security and protection toolkit replaces the NHS information governance toolkit as an online self-assessment tool that enables health and social care organisations, commissioners, IT suppliers and other relevant third parties to determine how securely the organisation manages their data. |
| Personal data | Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. |
| Privacy information | Information provided to individuals about the collection and use of their personal data. This must include purposes for processing their personal data, retention periods for that personal data, and who it will be shared with. This must be provided at the time personal data is collected. |
| Processing | Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Processor | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. This applies only to Journey 3 and Journey 4. |
| Publication scheme | The Freedom of Information Act 2000 provides the public access to official information held by public authorities. It requires every public authority to have a publication scheme, approved by the Information Commissioner’s Office (ICO), and to publish information covered by the scheme.  A publication scheme is a guide to the official information an organisation holds and routinely makes available such as who they are and what they do, how they spend their money etc. |
| Re-identification | The process of analysing data or combining it with other data with the result that individuals become identifiable. |
| Reasonable expectations | What a reasonable person would expect to happen, given the circumstances and information available to them. This is important to consider when relying on implied consent |
| Records of Processing Activity (RoPA) | Article 30 of GDPR states that each controller shall maintain a record of processing activities under its responsibilities. The Article details what should be contained in the record |
| Risk register | Data Protection Impact Assessments require an assessment of risks and measures to help mitigate those risks. A risk register is a tool which can support this by formally capturing the risk, information the nature, the owner and the mitigation of each risk |
| Role based access | Access to data is dependent on the role of the person so a receptionist would see different information to a consultant. |
| Secondary uses | This includes activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition. It also covers health services management, preventative medicine, and medical research. |
| Secondary Use Data Governance Tool (SUDGT) | A tool developed by NHS England to support Sustainable Transformation Partnerships/Integrated Care Systems to implement robust governance processes to support their uses of data, focused on data for secondary purposes. |
| Service level agreement (SLA) | An agreement negotiated between two parties where one is the customer and the other the service provider. The Service Level Agreement records a common understanding about services, priorities, responsibilities, guarantees and warranties. Service Level Agreements can be binding contracts but are often used by public sector bodies to set out their relationship in a given project without the intention to create legal relations. |
| Special category data | Personal data which the GDPR says is more sensitive, and so needs more protection. Such data includes health, genetic, biometric data. |
| Statutory functions | These functions that an organisation is legally required to do as set out in Acts of Parliament. |
| Subject access request (SAR) | Under GDPR Individuals have a right of access their personal data. This commonly referred to as a subject access request. |
| Third party | A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process data. |
| Threat | Any circumstance or event with the potential to adversely impact an asset through authorised access, destruction, disclosure, modification of data and/or denial of service. |
| Vital interests | Necessary to protect an interest which is essential for the life of the data subject or that of another natural person. |

## Appendix B – Using Health Data

**The new General Data Protection Regulation (GDPR) recital 4 states that:**

*The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and balanced against other fundamental rights, in accordance with the principle of proportionality.*

Recital 53 provides a broad definition of health and care purposes;

*Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health.*

**The ‘Information: To share or not to share?’ Information Governance Review in 2013 stated that;**

*People using health and social care services are entitled to expect that their personal information will remain confidential. They must feel able to discuss sensitive matters with a doctor, nurse or social worker without fear that the information may be improperly disclosed. These services cannot work effectively without trust and trust depends on confidentiality.*

*However, people also expect professionals to share information with other members of the care team, who need to co-operate to provide a seamless, integrated service. So good sharing of information, when sharing is appropriate, is as important as maintaining confidentiality. All organisations providing health or social care services must succeed in both respects if they are not to fail the people that they exist to serve.*

This led to the creation of a new Caldicott Principle;

*7. The duty to share information can be as important as the duty to protect patient confidentiality*

*Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.*

The Health and Social Care (Safety and Quality) Act 2015 [(Duty to Share)](http://www.legislation.gov.uk/ukpga/2015/28/pdfs/ukpga_20150028_en.pdf):

*Inserted section 251B of the Health and Social Care Act 2012 to introduce a new legal duty requiring health and adult social care bodies to share information in particular circumstances such as to facilitate care and where it is in the individual’s best interest. The precise conditions relied upon under the Data Protection Legislation will depend on whether this duty is engaged and the origin of the legal duties of the Controller. Clinicians must take into account any reasonable patient objections raised.*

## Appendix C - Governance Process

The LHCR Information Governance Framework will be developed and overseen by the National LHCR Information Governance Steering Group chaired by NHS England as part of the LHCR programme.

The National LHCR Information Governance Steering Group will report into the LHCR Programme Board.

An Information Governance Assurance Panel will be responsible for assessing assurance checkpoints. The Panel will consist of National information governance subject matter experts (NHS England, NHS Digital, NHS Improvement) and it is anticipated that representatives from the National Data Guardian (NDG), Understanding Patient Data (UPD), Health Research Authority (HRA), UK Caldicott Guardian Council, clinical representative, local authority /social care representative, patient representative, SIGN representative) will also join the Panel.

The LHCR Information Governance leads will be in regular contact with the National LHCR Information Governance Steering Group to raise issues or concerns and highlight best practice. They will meet as a group on a regular basis to discuss operation of the framework and to assist in developing tools, templates, models and share good practice.

Every LHCR will need to gain satisfactory assurance on each checkpoint before proceeding with data sharing across the LHCR member organisations. Where LHCR already has a shared local health and care record in place they should use the checkpoint to ensure themselves and the assurance panel that they are compliant. In the event that satisfactory assurance cannot be met support will be provided to achieve compliance.

## Appendix D – Definitions of Individual/Direct and Indirect Care

Both definitions are taken from “Information: To Share or not to Share? The Information Governance Review 2013”

**Definition of Individual care (Direct care)**

*A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals’ ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.*

D*irect care is provided by health and social care staff working in care teams, which may include doctors, nurses and a wide range of staff on regulated professional registers, including social workers. Relevant information should be shared with them when they have a legitimate relationship with the patient or service user.*

When sharing for direct care you need to be very clear about the purpose for which it is being used. If it does not fit into the above context it will not be considered individual care and therefore the way in which the information governance rules apply will change.

**Definition of indirect care (secondary uses)**

*Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of activities would be risk prediction and stratification, service evaluation, needs assessment, financial audit.*

## Appendix E – Lawful Conditions for Processing

**GDPR Article 6 and Article 9 applicable conditions**

**Article 6**

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;   
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

**Do not use consent as a condition for processing to meet GDPR/DPA requirements, unless in exceptional circumstances.[[14]](#footnote-15) The most appropriate basis for lawful processing that is available to publicly funded and/or statutory health and social care organisations in the delivery of their functions is Article 6(1)(c) or (e) and Article 9(2)(h) special category data (see Appendix E for further explanation). Where independent care providers are processing personal data in connection with the provision of self-funded care they can rely on Article 6(1)(f) (legitimate interests). There is no change to the Article 9 basis.**

**Article 9**

Conditions for processing of special categories of personal data:

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

1. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
2. Member states may maintain or introduce further conditions including limitations, with regard to the processing of genetic data, biometric data or data concerning health

**DPA 18 Chapter 2 applicable conditions**

Lawfulness of processing personal data set out in Article 6(1) (e) of the GDPR is covered under Section 8 of the DPA and covers situations where the processing is carried out in the public interest or where the controller is exercising ‘official authority’ including but not limited to:

(a) the administration of justice,   
(b) the exercise of a function of either House of Parliament,   
(c) the exercise of a function conferred on a person by an enactment or rule of law,   
(d) the exercise of a function of the Crown, a Minister of the Crown or a government department, or   
(e) an activity that supports or promotes democratic engagement.

The lawfulness of processing special categories of personal data set out in Article 9 (2)(h) of GDPR is covered under Section 10 and 11 of DPA 2018 and the processing meets the following conditions set out in Part 1 of Schedule 1 of the Act:

The processing is necessary for “health or social care purposes”, these mean the purposes of:

1. preventive or occupational medicine,
2. medical diagnosis,
3. the provision of health care or treatment,
4. the provision of social care, or
5. the management of health care systems or services or social care systems or services

Special categories of personal data etc: DPA 2018 supplementary

For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of special categories of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of professional secrecy) include circumstances in which it is carried out:

1. by or under the responsibility of a health professional or a social work professional, or
2. by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

**DPA (2018) s204 - Meaning of “health professional” and “social work professional”**

(1) In this Act, “health professional” means any of the following—

(a)a registered medical practitioner;

(b)a registered nurse or midwife;

(c)a registered dentist within the meaning of the Dentists Act 1984 (see section 53 of that Act);

(d)a registered dispensing optician or a registered optometrist within the meaning of the Opticians Act 1989 (see section 36 of that Act);

(e)a registered osteopath with the meaning of the Osteopaths Act 1993 (see section 41 of that Act);

(f)a registered chiropractor within the meaning of the Chiropractors Act 1994 (see section 43 of that Act);

(g)a person registered as a member of a profession to which the Health and Social Work Professions Order 2001 ([S.I. 2002/254](http://www.legislation.gov.uk/id/uksi/2002/254)) for the time being extends, other than the social work profession in England;

(h)a registered pharmacist or a registered pharmacy technician within the meaning of the Pharmacy Order 2010 ([S.I. 2010/231](http://www.legislation.gov.uk/id/uksi/2010/231)) (see article 3 of that Order);

(i)a registered person within the meaning of the Pharmacy (Northern Ireland) Order 1976 ([S.I. 1976/1213 (N.I. 22)](http://www.legislation.gov.uk/id/nisi/1976/1213)) (see Article 2 of that Order);

(j)a child psychotherapist;

(k)a scientist employed by a health service body as head of a department.

(2)In this Act, “social work professional” means any of the following—

(a)a person registered as a social worker in England in the register maintained under the Health and Social

Work Professions Order 2001 ([S.I. 2002/254](http://www.legislation.gov.uk/id/uksi/2002/254));

(b)a person registered as a social worker in the register maintained by Social Care Wales under section 80 of the [Regulation and Inspection of Social Care (Wales) Act 2016 (anaw 2)](http://www.legislation.gov.uk/id/anaw/2016/2);

(c)a person registered as a social worker in the register maintained by the Scottish Social Services Council under section 44 of the Regulation of Care (Scotland) Act [2001 (asp 8)](http://www.legislation.gov.uk/id/asp/2001/8);

(d)a person registered as a social worker in the register maintained by the Northern Ireland Social Care Council under section 3 of the [Health and Personal Social Services Act (Northern Ireland) 2001 (c. 3 (N.I.))](http://www.legislation.gov.uk/id/nia/2009/1).

(3)In subsection (1)(a) “registered medical practitioner” includes a person who is provisionally registered under section 15 or 21 of the Medical Act 1983 and is engaged in such employment as is mentioned in subsection (3) of that section.

(4)In subsection (1)(k) “health service body” means any of the following:—

(a)the Secretary of State in relation to the exercise of functions under section 2A or 2B of, or paragraph 7C, 8 or 12 of Schedule 1 to, the National Health Service Act 2006;

(b)a local authority in relation to the exercise of functions under section 2B or 111 of, or any of paragraphs 1 to 7B or 13 of Schedule 1 to, the National Health Service Act 2006;

(c)a National Health Service trust first established under section 25 of the National Health Service Act 2006;

(d)a Special Health Authority established under section 28 of the National Health Service Act 2006;

(e)an NHS foundation trust;

(f)the National Institute for Health and Care Excellence;

(g)the Health and Social Care Information Centre;

(h)a National Health Service trust first established under section 5 of the National Health Service and Community Care Act 1990;

(i)a Local Health Board established under section 11 of the National Health Service (Wales) Act 2006;

(j)a National Health Service trust first established under section 18 of the National Health Service (Wales) Act 2006;

(k)a Special Health Authority established under section 22 of the National Health Service (Wales) Act 2006;

(l)a Health Board within the meaning of the National Health Service (Scotland) Act 1978;

(m)a Special Health Board within the meaning of the National Health Service (Scotland) Act 1978;

(n)a National Health Service trust first established under section 12A of the National Health Service (Scotland) Act 1978;

(o)the managers of a State Hospital provided under section 102 of the National Health Service (Scotland) Act 1978;

(p)the Regional Health and Social Care Board established under section 7 of the [Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I))](http://www.legislation.gov.uk/id/nia/2009/1);

(q)a special health and social care agency established under the Health and Personal Social Services (Special Agencies) (Northern Ireland) Order 1990 ([S.I. 1990/247 (N.I. 3)](http://www.legislation.gov.uk/id/nisi/1990/247));

(r)a Health and Social Care trust established under Article 10 of the Health and Personal Social Services (Northern Ireland) Order 1991 ([S.I. 1991/194 (N.I. 1)](http://www.legislation.gov.uk/id/nisi/1991/194)).

## Appendix F – Common Law

Common law (case law) is law that has developed through the courts making decisions on legal points in specific cases and creating binding precedents. It differs from statutory law, which is determined by acts of parliament.

Essentially, the common law duty of confidentiality means that when someone (such as a patient) shares personal information in confidence (to a health care professional, for example) it must not be disclosed without some form of legal authority or justification. In practice, this usually means that the information cannot be disclosed without that person’s consent — unless there is another valid legal basis, such as a court order, or overriding public interest. Where a patient has agreed to a programme of treatment and care then it is assumed that they have agreed to the use of their CPI to support that programme, this is known as implied consent.

In certain situations, for example for research, approval from the Health Research Authority (HRA) may be obtained under Section 251 of the National Health Service Act 2006, on the recommendation of the HRA’s Confidentiality Advisory Group (CAG).

## Appendix G - Consent and applicable GDPR Recitals

**Do not use consent as a condition for processing to meet GDPR/DPA requirements, unless in exceptional circumstances [[15]](#footnote-16) The most appropriate basis for lawful processing that is available to publicly funded and/or statutory health and social care organisations in the delivery of their functions is Article 6(1)(e)’…for the performance of a task carried out in the public interest or in the exercise of official authority…..’**

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (1) a declaration of consent pre- formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

## Appendix H – Supporting Tools and Templates

Please see separate document for this appendix.

## Appendix I – GDPR Article 21 – Right to Object

1. 1The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of [Article 6(](https://gdpr-info.eu/art-6-gdpr/)1), including profiling based on those provisions. 2The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding [Directive 2002/58/EC](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058), the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to [Article 89(](https://gdpr-info.eu/art-89-gdpr/)1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

## Appendix J – GDPR Article 26 – Joint Controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in [Articles 13](https://gdpr-info.eu/art-13-gdpr/) and [14](https://gdpr-info.eu/art-14-gdpr/), by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.
2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

**Joint Data Controllership – ICO thinking**

There is now a clear distinction between controllers working together as joint controllers or alone as individual controllers. LHCRs will be joint controllers, as between them they will decide on the purpose and manner for which personal data is collected; it will not be decided by one single organisation within the LHCR; as a LHCR is not a legal entity, joint controllers will need to enter into binding contracts/processing agreements with data processers as a “group” of data controllers rather than appoint a single lead data controller to act on behalf of the group.

**The below gives the ICO thinking with regards to Data Controllership for both enhanced sharing and combined record and therefore how Joint Controllership for LHCR’s determined.**

**‘Enhanced sharing’** – no external record just method which allows distinct controllers to get record from wherever it held.

**‘Combined record’** – each organisation contributing to a centrally shared record all have access to.

Whilst being a relatively basic tool the [online checklist](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/) does provide some insight into the factors to consider when determining if you’re acting ‘jointly’. It may be useful to illustrate the point that **a shared purpose is only one factor**;

Are we a joint controller? (The more you tick the more likely you are)

* We have a common objective with others regarding the processing.
* We are processing the personal data for the same purpose as another controller.
* We are using the same set of personal data (e.g. one database) for this processing as another controller.
* We have designed this process with another controller.
* We have common information management rules with another controller

**Enhanced sharing** – the enhanced sharing type arrangement could be described as a controller to controller arrangement as there is no ‘joint purpose’, however looking at the ICO checklist you could still have;

* Common objective – linked up care, correct info and not having to ask patient every time
* Same set of personal data
* Designed this process with another controller – all LHCRs work together to establish system
* Although might use different policies organisations still form part of a wider framework as most organisations will want to assure the compliance of others within the LHCRE (DSP toolkit, DP laws, LHCR framework agreement, common training requirements?)

**Combined model** – this isn’t controller-to-controller as a joint record is created that requires ownership but similar factors established;

* Common objective – linked up care records, correct info and not having to ask patient every time
* Purpose – in creating the record they’re establishing a purpose for the creation of joint record.
* Same set of personal data
* Designed this process with another controller – all’s LHCRs work together to establish system?
* Although might use different organisations policies still within a wider framework as most organisations will want to assure the compliance of others in LHCRE (DSP toolkit, DP laws, LHCR framework ) (\***This is a broad interpretation on this point**)

## Appendix K – Security Requirements

**2017/18 Data Security and Protection Requirements**

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/675420/17-18_statement_of_requirements_Branded_template_final_22_11_18-1.pdf>

Covers NHS organisations, General Practice, Local Government and Social Care Providers

**GP IT Operating Model Addendum 2018/19**

<https://www.england.nhs.uk/publication/2018-19-addendum-to-the-gp-it-operating-model-securing-excellence-in-gp-it-services-2016-18-revisions/>

The addendum, references various other documents, including:

* Your Data: Better Security, Better Choice, Better Care: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/627493/Your_data_better_security_better_choice_better_care_government_response.pdf>
* 2017/18 Data Security and Protection Requirements: (link as above)
* 2017/18 General Medical Services Digital Guidance issued jointly by NHS England and the General Practitioners Committee (GPC): <https://www.england.nhs.uk/wp-content/uploads/2017/04/17-18-gms-digital-guidance.pdf>

In addition NHS Providers (and a number of independent providers) are classed as Operators of Essential Services and will be subject to the Network and Information Systems (NIS) Regulations <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/706613/network-and-information-systems-regulations-2018-health-sector-guide.pdf>

Regarding tools, templates and assurances, there is an expectation that health and care organisations will be addressing relevant recommendations in the CIO Review <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf> Certification to standards such as Cyber Essentials Plus (for organisations that partner to form the LHCR) is recommended. Reporting of compliance and any breaches will be via the Data Security Protection Toolkit (which replaced the IG Toolkit from 1st April 2018).

It should be noted that local authorities are not mandated to certify to standards such as Cyber Essentials and, Cyber Essentials Plus. However, they will need to meet the requirements of the Data Security and Protection toolkit as part of the process to get a NHS connection, to be able to access NHS systems or data which is relevant for Adult Social Care. In addition, Local Authorities demonstrate their organisations’ security arrangements, policies and controls are sufficiently rigorous through compliance against a set of assertions within the Code of Connection for the Public Service Network (PSN)

## Appendix L - 2017/19 NHS Standard Contract[[16]](#footnote-17)

Where a Local Authority commissions an NHS agency (The Provider) to deliver its Child and Adolescent Mental Health Services (CAMHS) using the NHS Standard Contract, the Local Authority still retains its duty to respond to statutory complaints

GC21.12 of the Standard Contract states that *where a commissioner requires information for “quality management of care processes” (this includes handling complaints about the Provider), the NHS Agency must consider whether the request can be met by anonymised or aggregated data and where personal data is required, ensure there is a legal basis.* This legal basis can be found in GDPR which doesn’t distinguish between commissioners and providers: - Public Task (Art 6) providing the conditions of Art 9(3) are met, under the responsibility of a clinical or social work professional (as listed in DPA 2018 S204

## Appendix M - Assurance Checkpoint Matrix (for completion by the LHCREs)

* The Checklist is intended to provide assurance to LHCREs that they are following the guidance outlined in the Framework
* Each requirement has the associated assurance checkpoints in the associated rows across the page e.g: “Structure requirement” ~ the associated checkpoints (evidence) are 1.1, 1.2, 1.3, 1.4.
* LHCRs to use the checklist to self-assess the evidence. (Satisfactory evidence is ticked in the appropriate cell).
* After the self-assessment is complete and the LHCR feels ‘ready’, it can make submission to the IG Assurance Panel for assurance.
* The LHCR must submit papers to the Panel Administrator **no later than 15 days prior to the Panel meeting**. The papers will include a covering letter from the LHCR (see template), a signed off copy of the Assurance Checklist Matrix and the supporting evidence detailed within the Matrix.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement (IG Framework)** | **Assurance Checkpoint (Evidence)** | **Checkpoint Notes** | **Is there satisfactory evidence?** (tick, for ‘yes’) | **LHCR comments** |
| 1. **Structure**   Each LHCR has a consistent approach to IG policy, processes and systems and is part of an IG structure which ensures good IG practice across the LHCR. | * 1. 1.1 Appointment of a LHCR IG Lead (subject matter expert) | N/A |  |  |
| * 1. 1.2 LHCR IG Lead is a member of the LHCR IG Leads Network and attends national strategic IG meetings | N/A |  |  |
| * 1. 1.3 Structure chart for LHCR Information Governance and communication input | N/A |  |  |
| 1.4 Evidence of information Governance policies | N/A |  |  |
| 1. Legal Requirements   Each LHCR understanding how participating organisations meets the legal requirements to process confidential patient information, including statutory basis, conditions for processing and considerations under the Common Law Duty of Confidence | 2.1 Evidence of a statement for each organisation involved in the collective sharing setting out the purpose, lawful basis for processing, duty of confidence satisfied | N/A |  |  |
| 2.2 LHCR will have a Privacy Notice stating what data is collected, stored, shared and retained and for how long. The Privacy Notice must also include information on patient preferences | NB. This evidence (Privacy Notice) relates to two checkpoints: 2.2, 3.1 |  |  |
| 2.3 Agreed approach across each LHCR for the management of patient objections to share their data for individual care | NB. This evidence relates to two checkpoints: 2.3, 8.3 |  |  |
| 2.4 Evidence of effective Role Based Access Control (RBAC) | NB. This evidence (RBAC) relates to two checkpoints: 2.4, 7.7 |  |  |
| 2.5 Evidence of completed and approved DPIA for each data sharing purpose | NB. This evidence (DPIA) relates to three checkpoints: 2.5, 7.3, 9.1 |  |  |
| 1. **Duty of Transparency**   LHCRs need to demonstrate that they are meeting the duty of Transparency. This is one of the ways that LHCRs can build trust and gain public respect in use of their data. In addition, it supports the GDPR principle of accountability which organisations need to demonstrate compliance. | * 1. 3.1 Privacy Notice(s) stating what data is collected, stored, shared and retained (for how long). The Privacy Notice must also include information on patient preferences | NB. This evidence (Privacy Notice) relates to two checkpoints: 2.2, 3.1 |  |  |
| 3.2 Production of a clear plan, list of communication materials and channels | NB. This evidence relates to two checkpoints: 3.2, 3.5 |  |  |
| 3.3 Copies of the information provided to the public/ patients | NB. This evidence relates to two checkpoints: 3.3, 3.4 |  |  |
| 3.4 Evidence of publication of transparency materials by all organisations in the LHCR | NB. This evidence relates to two checkpoints: 3.3, 3.4 |  |  |
| 3.5 Details of the process of monitoring and updating communications | NB. This evidence relates to two checkpoints: 3.2, 3.5 |  |  |
| 3.6 Evidence of publication of information to the public such as Records of Processing, sharing agreements | N/A |  |  |
| 3.7 Adoption of online access capability and ability to demonstrate update (if available) | N/A |  |  |
| 3.8 Evidence of public engagement to gain their view of the approach and test materials | N/A |  |  |
| 1. **Data Flows and Controllership** | * 1. 4.1 Evidence of Data Sharing Agreements/ Protocols for the grouping | NB. The evidence (DSA) relates to two checkpoints: 4.1, 7.4 |  |  |
| * 1. 4.2 A written contract between the grouping and the processor/s | N/A |  |  |
| 4.3 A clear data processing map showing purpose and Data Controller/ Data Processor at each stage of the data flow. | N/A |  |  |
| 4.4 Each LHCR has the required Service Level Agreements | N/A |  |  |
| 4.5 Each LHCR use standard contract clauses | N/A |  |  |
| 1. **Records of Processing Activity. Art 30**   Organisations (which are public bodies) need to be clear that the processing that they wish to undertake matches their statutory functions. They are to produce and maintain Records of Processing Activity (RoPA) as part of legal compliance.  These statutory functions and legislation should also be identified and published in the Information Asset | * 1. 5.1 Evidence of Records of Processing Activity / Production of an Information Asset register | N/A |  |  |
| 5.2 Evidence of policies and procedures for information asset management | N/A |  |  |
| 1. **Assuring Security**   within the LHCR comply with relevant legislation and adhere to current published guidance for health and care and, develop cyber security to protect the confidential | 6.1 Publication and evidence of compliance with policies for areas such as staff training, internal audit, HR policies, retention and disposal schedules. | N/A |  |  |
| 6.2 Evidence of annual completed and (where there is mandatory requirement) audited Data Security and Protection Toolkit to meet the mandated requirements (e,g, Records of Processing Activities are documented, cyber assurance) | N/A |  |  |
| 6.3 Evidence of Board approved action plan **IF** the mandated requirements are not met | N/A |  |  |
| 6.4 Evidence of independent onsite assessments | N/A |  |  |
| 6.5 Evidence of organisations signed up to receive cyber threat intelligence from CARECERT. | N/A |  |  |
| **7.0 Data Access, Review, Retention**  LHCRs need to have audit functionality which enables controllers to meet their access control responsibilities | 7.1 Data Maps | N/A |  |  |
| 7.2 Data Processing Contract | N/A |  |  |
| 7.3 Evidence of completed and approved Data Protection Impact Assessment (DPIA) for each data sharing purpose | NB. This evidence (DPIA) relates to three checkpoints: 2.5, 7.3, 9.1 |  |  |
| 7.4 Data Sharing Agreement (DSA) | NB. The evidence (DSA) relates to two checkpoints: 4.1, 7.4 |  |  |
| 7.5 Evidence of compliance with Records Management Code of Practice for Health and Social Care 2019 | N/A |  |  |
| 7.6 Policies and Audit | N/A |  |  |
| 7.7 Evidence of effective Role Based Access Control (RBAC) | NB. The evidence (RBAC) relates to two checkpoints: 2.4 , 7.7 |  |  |
| **8.0 Individual Rights**  LHCRs need to be clear on which individual rights apply and have processes in place to ensure an individual can enact those rights | 8.1 Evidence of process in place for complying with individual rights where required.ie. rectification, objection, subject access request | N/A |  |  |
| 8.2 Evidence of how patients can exercise individual rights in transparency documentation | N/A |  |  |
| * 1. 8.3 Agreed approach to managing patient objections to share their data for individual care under the LHCR | NB. The evidence relates to two checkpoints: 2.3, 8.3 |  |  |
| **9.0 Demonstrating Accountability**  Each LHCR to ensure that DPIA is undertaken to identify any risks to the processing of personal data | 9.1 Evidence of completed and approved DPIA for each data sharing purpose | NB. This evidence (DPIA) relates to three checkpoints: 2.5, 7.3, 9.1 |  |  |
| 9.2 Evidence of Information Governance considerations in Project Initiation Documentation | N/A |  |  |
| 9.3 Evidence of DPIA risks incorporated into (organisational/LHCR) risk register including mitigation and management | N/A |  |  |
| 9.4 Evidence of consultation with the public on the DPIA | N/A |  |  |
| 9.5 Evidence that unmitigated high risks are escalated to the DPO and the ICO is consulted | N/A |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Signed off by Internal Audit | Name: |  | Signature: |  | Date: (dd/mm/yyyy): |  |
| Signed off by the Board | Name: |  | Signature: |  | Date (dd/mm/yyyy): |  |

## Appendix N - Individual Rights under GDPR - Art. 12 - 23

* + - 1. **The right to be informed**

The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing individuals with clear and concise information about what you do with their personal data. (Articles 13 and 14 specify what individuals have the right to be informed about)

* + - 1. **The right of access**

Individuals have the right to access their personal data which is commonly referred to as a “Subject Access Request”. Responses to these requests should typically be made within one month (however there are circumstances where an extension may be sought). There needs to be consideration if the request includes information about others.

* + - 1. **The right to rectification**

Individuals have a right to have inaccurate personal data rectified, or completed if it is incomplete. These requests can be made verbally or in writing and organisations have one calendar month to respond. In certain circumstances, organisations can refuse a request for rectification. (Note, this right is closely linked to controllers obligations under the accuracy principle of GDPR [Article (5) (1) (d)].

Please note the following relevant statements from the NHS Constitution (2013, 2015) and how this right may be applied:

*“You have the right to have any factual inaccuracies corrected. Ask your health professional about amending your records if you believe they contain a factual error.”*

*“There is no obligation to amend professional opinion however sometimes it is difficult to distinguish between fact and opinion. Where you and the health professional cannot agree on whether the information in question is accurate, you can ask that a statement is included to set out that the accuracy of the information is disputed by you”*

(pg 56) The Handbook to the NHS Constitution 2013:

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/170649/Handbook_to_the_NHS_Constitution.pdf>

The NHS Handbook 2015 states that: “*You have the right of access to your own health records and to have any factual inaccuracies corrected.”*

Ref: (pg8) The Handbook to the NHS Constitution 2015 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/480482/NHS_Constitution_WEB.pdf>

1. **The right to erasure**

Individuals have a right to have certain personal data erased commonly known as “the right to be forgotten”. This request can be made verbally or in writing. Organisations have one month to respond to a request. This right is **not** an absolute and only applies in certain circumstances. The NHS European Office explain that “the right to be forgotten and erasure of data does not apply to an individual’s health record, or for public health purposes or research purposes.” Clinicians may advise patients that certain data cannot be removed because it allows continuity of care for their wellbeing. An alternative is that where appropriate

Relevant **exemptions** include if the data collection took place to comply with legal obligations or in the exercise of official authority for the public interest.

A general public interest exemption also exists for archiving purposes in the public interest and, for scientific research purposes and statistical purposes as well

This right only applies where data is processed under consent.

1. **The right to restrict processing**

Individuals have the right to request the restriction or suppression of their personal data. This request can be made verbally or in writing. Organisations have one calendar month to respond to a request. This is not an absolute right and only applies in certain circumstances. When processing is restricted, organisations are permitted to store the data but not use it.

This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

1. **The right to data portability**

This right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure manner, without affecting its usability. This right only applies to information that the individual has provided to the controller.

**Please note** this applies if the data processing is automated, and the legal justification is consent. I.e. where the organisation’s lawful basis is public interest (task) then rights of portability do not apply.

1. **The right to object**

Individuals have the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. They can make this objection verbally or in writing and organisations have one calendar month to respond to an objection.

There are other cases where organisations can continue processing the data, if they show that they have a compelling reason for doing so.

1. **Rights in relation to automated decision making and profiling.**

The GDPR has provisions on:

* + automated individual decision-making (making a decision solely by automated means without any human involvement); and
  + profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Article 22 of the GDPR has additional rules to protect individuals if organisations are carrying out solely automated decision-making that has legal or similarly significant effects on them.  These types of effect are not defined in the GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision.

**Please note:**  There are exemptions such as where automation is in accordance with another law, where the automation is necessary for the entering or performance of a contract between the individual and pharmacy contractor, or when the individual has given their explicit consent.

## Appendix O – Data Breach Management

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The General Data Protection Regulation 2018 introduces a duty on all organisations to investigate security incidents to establish whether a personal data breach has occurred and so will need to have robust breach detection, investigation and internal reporting procedures in place.

If a personal data breach has occurred, organisations need to promptly take steps to address this including reporting certain types of personal data breaches to the relevant supervisory authority. In these cases, reporting must be done within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, organisations must also inform those individuals without delay.

Organisations must keep a record of all personal data breaches regardless of whether or not these are reported to the supervisory authority.

Any breaches that also fulfil the criteria of a “Security of Network and Information Systems” (NIS)[[17]](#footnote-18) notifiable incident will be forwarded to the DHSC where the Secretary of State is the competent authority for the implementation of the NIS directive in the health and social care sector. The Information Commissioner remains the national regulatory authority for the NIS directive.)

**Useful documents and Guidance:**

The **“****Data Security Standard 6: Guide to the Notification of Data Security and Protection Incidents[[18]](#footnote-19)”** written by NHS Digital sets out different types of breaches, when a breach is reportable and, incident management & breach reporting process.

The guide is written for all organisations operating in the health and care sector (including organisations registered with Care Quality Commission (CAC) and those organisations processing health and social care personal data under contract with the health and social care sector including directly commissioned services and their support services). In these cases, breaches are reported using the Reporting Tool within the DSPT.

However, other organisations such as private health and social care services that are not contracted by a public-sector organisation and those parts of local government not delivering adult social care services can also use the Reporting Tool within the DSPT.

Any personal data breaches that fall out of scope can be reported either via this reporting tool or to the Information Commissioner directly at the discretion of the reporting organisation.

The Information Commissioners Office has produced some useful guides on their website which sets out a data breach management/ reporting process:

Security Breaches: <https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/>

Personal Data Breaches: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

## Appendix P – Role Based Access Control (RBAC)

LHCRs need to demonstrate access control as relates to the use of confidential patient information. Patients have the right to know who has access rights and has accessed their record for processing. They also have the right to challenge that access. This is a fundamental principle and essential for maintaining public trust.

LHCRs need to ensure that only health and care professionals who have a **legitimate relationship** with the patient, in the delivery of their care, will have access to their patient record. This will ensure that the level of access to confidential patient information is “necessary and proportionate”.

Role Based Access Control (RBAC) is an effective model to support appropriate data sharing across the LHCRs - the health or care professional who has a **legitimate relationship** with the patientwill have access to the appropriate level of data required to deliver safe care.

“System roles” set up within RBAC allow different levels of data access and type of access (whether read only, read-write access). Organisations operating within the LHCR will need to assign staff to “system role(s)” relevant for their job role of the staff. For example, those working as a registered and regulated health or social care professional will have “fullest access” to patient clinical data**,** to ensure that treatments are informed by the best available information about the patient reducing the risk of inappropriate interventions. Professionals that fall within “health professional” and “social work professional” are defined in [Data Protection Act 2018 (Section 204)](http://www.legislation.gov.uk/ukpga/2018/12/section/204/enacted) and also [NHS Confidentiality Guide (Section 7)](https://webarchive.nationalarchives.gov.uk/20180328130852tf_/http:/content.digital.nhs.uk/media/12823/Confidentiality-guide-References/pdf/confidentiality-guide-references.pdf/).

Whilst registered and regulated social workers should be considered equivalent to registered and regulated healthcare professionals, “fullest access” **must** be appropriate for the specialism. The needs of each specialism should be considered to determine what the minimum data set needed to provide safe care. These requirements would be enabled through an effective RBAC.

Staff will only be able to access data, that their “system role(s)” permits. Thus typically a receptionist will not have the same level of access as a clinician.

**Legitimate Relationship**

Legitimate relationship is an important concept that needs to be considered as part of access control. The Information Governance Review 2013 defines “Legitimate relationship” as *“the legal relationship that exists between an individual and the health and social care professionals and staff providing or supporting their care*[[19]](#footnote-20)” LHCRs need to ensure that only health and care professionals who have a legitimate need to see the patient’s record can see information about the patient.

A legitimate relationship is created by a patient event and it is only whilst the legitimate relationship exists that the patient record should be accessed by the clinician or appropriate personnel.

**Role based access** (which controls the level of data access that the professional can see on the patient record) and **legitimate relationship** (which confirms whether there is a reason why the patient record is accessed by the said professional). Together, these both help to demonstrate access control to confidential patient information.

Legitimate relationship is triggered by patient events and will support reasons why access is required to the patient record. Some examples are listed below:

1. **Patient Referral/ Request:** A legitimate relationship is created when a referral or service request is made. Some examples are:

* A referral between consultants in a hospital
* A request for a laboratory test;
* booking an appointment for a patient
* an admission to a hospital ward;
* when a member of staff requests a service from another member of staff or team on behalf of the patient

1. **Patient Self-Referral**:A legitimate relationship is created when a patient attends Accident & Emergency and upon registering when they enter. This will create a self-referral legitimate relationship and this will enable clinical staff to view the patients record. Similarly, if a patient attends a walk-in clinic, this is a self-referral and again a patient self-referral legitimate relationship can be created between the patient and the workforce group providing the service in question.
2. **General Practice Registration:** When a patient registers with a new general practitioner, a legitimate relationship is created. Clinicians will be entitled to access clinical record by using the legitimate relationship created when the patient registered. Also, administrators working in a general practice need access to limited clinical information about the patient, and so the Legitimate Relationship created at registration must allow for this.
3. **Patient Registration:** Legitimate relationships will be applied to other situations such as registration with NHS Dentistry, screening and other situations where patients are added and removed from a well-defined, registered service
4. **Subject Access Requests:**  Under GDPR, an individual has a right of access and this subject access request must be processed within a set time frame and provide the subject of the request with a copy of all the personal data held within their record. A legitimate relationship may be created through receiving this request particularly if in a general practice setting, the patient has left the practice. This is only for the length of time that it takes to process the SAR.
5. **Patient Complaint or Litigation:** When a patient complains or begins litigation with respect to some aspect(s) of the service that they receive from an NHS organisation, their complaint must be investigated. Some complaints that do not have anything to do with the care received will not require access to a patient clinical record, so no legitimate relationship will be created. Where patients submitting complaints are unhappy with the clinical care that they have received, these complaints will need to be properly investigated and will require access to relevant information within the patient clinical record. Therefore, when the complaint is received and recorded in the system, a legitimate relationship is created between the patient and the team (work group) carrying out the investigation.
6. **Self-Claimed:** In occasions where a care professional is denied access to the patient record because there is no existing legitimate relationship but there is an urgent need to view the patient record, if they have sufficient authorisation, they will be able to gain access to the patient record through the creation of a self-claimed legitimate relationship. This is only for a limited time and justification would need to be recorded. If a member of staff is found to have self-claimed inappropriately, they will need to face disciplinary procedures
7. **Colleague-Granted**: if acare professional wants to ask a colleague for a second opinion about a patient, and agrees this with the patient. However, if the colleague works in a different Workgroup, he or she is unlikely to have a Legitimate Relationship with the patient. In such circumstances, the patient's doctor can create a Colleague-Granted Legitimate Relationship to provide the colleague with access to the patient’s clinical record.
8. **Court Order:** A court may demand information from a patient’s clinical record. This will require someone from an NHS organisation to access the patient’s clinical record. In this case, a legitimate relationship will be established between patient and the workgroup allowing for relevant information to be accessed and extracted from the patient record to satisfy the court.

**Audit**

An effective RBAC will allow organisations to be able to audit who has accessed a patient record. This is an important for transparency and to build patient trust.

Patients have the right to know who has access rights to their patient record, who has accessed their patient record for processing. Patients can challenge the access and if a complaint is received, this will require reactive and targeted auditing to response to specific concerned.

Where an incident is identified, organisations would be able to determine if the individual who accessed the patient record had correctly claimed a legitimate relationship. If data access is deemed to have been inappropriate, organisations must take the necessary remedial and/or disciplinary action.

Organisations should also undertake regular auditing to confirm that all users have the correct access rights assigned to them.

## Appendix Q – Patient Preferences Template Text

It would be helpful if LHCRs were using similar language when describing these different options (e.g. on websites) to avoid confusion when patients move between LHCRs and hence some template text is provided below:-

**Right to object**

You have a legal right to object to your data being shared. Your objection will be considered on a case by case basis.  When considering your objection, we  will consider whether you can still be provided with safe individual care.  Please contact [*X*] to discuss this further.

**Opt-out [option]**

Health and care staff use your confidential patient information to help with your treatment and care.  For example, when you visit a hospital your consultant may need to know the medicines you take.   To opt out please [*e.g. complete the following form*].  You will be opting out of having a Local Health and Care Record.    This is separate to the Summary Care record [*embed link* [*https://digital.nhs.uk/services/summary-care-records-scr/summary-care-records-scr-information-for-patients*](https://digital.nhs.uk/services/summary-care-records-scr/summary-care-records-scr-information-for-patients)] and [*list other local opt-outs with links where possible*] - you should continue to opt out of them separately.

**Asking to view [option]**

We will ask you before accessing your record.

**Your Data Matters to the NHS**

Information about your health and care helps us to improve your individual care, speed up diagnosis, plan your local services and research new treatments.

You can choose whether your confidential patient information is used for research and planning.  To find out more visit: [nhs.uk/your-nhs-data-matters](http://nhs.uk/your-nhs-data-matters)

**[Option]**

You may also be asked to give your consent to be involved in specific research studies. In [area] you can give your consent to be involved in [*information about the local project where consent is being sought including benefits*]

1. Individual Care has the same meaning as Direct Care, as defined in the Caldicott 2 Review 2013. [↑](#footnote-ref-2)
2. A Summary document is available here: <https://www.england.nhs.uk/wp-content/uploads/2018/05/local-health-and-care-record-exemplars-summary.pdf> [↑](#footnote-ref-3)
3. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF> [↑](#footnote-ref-4)
4. <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance>  
   This GDPR guidance includes the GDPR and Consent. [↑](#footnote-ref-5)
5. Primary care providers operating under contract with NHS England do not have direct legal authority. The authority rests with NHS England. However, where services are provided under such contracts, the providing bodies are subject to statutory regulation and can therefore rely on Art. 6 (1)(c). Any service provided beyond the contract will be covered by Art. 6(1)(e). [↑](#footnote-ref-6)
6. Recital 38 GDPR states additional protections need to be given to children in relation to marketing, creating a personality or user profile, or when offering services directly to a child.

   See also <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/> [↑](#footnote-ref-7)
7. For more guidance on Data Controllers and Processors, visit <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/> [↑](#footnote-ref-8)
8. https://www.dsptoolkit.nhs.uk/ [↑](#footnote-ref-9)
9. GPs also sign a contract allowing the CCG to procure a system on their behalf, and the CCG signs a contract with the supplier of choice, to enable them to call off products on behalf of its member practices. [↑](#footnote-ref-10)
10. https://www.dsptoolkit.nhs.uk/Help/Attachment/24 [↑](#footnote-ref-11)
11. <https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf> [↑](#footnote-ref-12)
12. See ICO’s Anonymisation Code of Practice. LCHREs should follow this as a basis for anonymising data for secondary use. The Code remains extant until replaced by an updated version (the Code is currently being reviewed by the ICO). When new guidance is published, guidance for LHCRs will be reviewed and updated. [↑](#footnote-ref-13)
13. <https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/> [↑](#footnote-ref-14)
14. <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance>  
    This GDPR guidance includes the GDPR and Consent. [↑](#footnote-ref-15)
15. See: <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance>  
    This GDPR guidance includes the GDPR and Consent. [↑](#footnote-ref-16)
16. <https://www.england.nhs.uk/nhs-standard-contract/2017-19-update-may/>) [↑](#footnote-ref-17)
17. The Security of Network and Information Systems Directive (NIS Directive) 2018 requires the reporting of relevant incidents to the Department of Health and Social Care (DHSC) as a competent authority [↑](#footnote-ref-18)
18. <https://www.dsptoolkit.nhs.uk/(X(1)S(5aqfcbbwqnobxiuykxwjez3s))/Help/Attachment/148> [↑](#footnote-ref-19)
19. [Information governance review 2013 "To Share or Not to Share" pg 129](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf) [↑](#footnote-ref-20)