Information Governance Framework for Integrated Health and Care: Shared Care Records

SEPTEMBER 2021

CONTENTS

Executive summary

The aim of Shared Care Records (ShCR) 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 record is shared across the health and care system. This will help health and care professionals to use information safely and securely as the people they care for move between different parts of the NHS and social care. It will also enable patients and service users to access their record irrespective of where they receive care.

ShCR was formerly known as the Local Health and Care Record (LHCR) programme. For the ShCR/LHCR programme, exemplar areas were identified. Other ShCR geographies are being onboarded to ensure full national coverage. The exemplar areas are:

- OneLondon
- Yorkshire and Humber
- Thames Valley and Surrey
- Greater Manchester
- Wessex

The Information Governance (IG) Framework is intended for IG professionals. It has been developed to provide a structured approach to ensure ShCRs meet their legal obligations. This includes when they are planning, preparing and delivering data sharing.

It is based on a model where controllership continues to remain local. Local agreements will be in place to set out what data is shared and who can access it in a safe, secure and appropriate manner. This approach recognises the variance in how data is captured and represented in local systems.

ShCRs will initially focus on individual care. This is covered in two journeys:

- **Journey 1:** Sharing personal/confidential patient information (CPI) between health and social care bodies within a ShCR for the individual care of patients or service users.
- **Journey 2:** Sharing personal/CPI between health and social care bodies across geographical boundaries for the individual care of patients or service users.

The following requirements are essential for IG compliance and good practice and need to be considered for both journeys.

Each ShCR should:

1. have a consistent approach to IG policies, processes and systems to ensure good practice
2. identify the flows of data, and at each point in the process to determine who the controllers and/or processors are
3. identify and understand the legal basis for processing data for every function including ensuring transparency about purpose and process, supporting good practice, and promoting public engagement
4. manage access controls and records management
5. consider patient and service user objections to processing
6. adhere to current published guidance on cyber security for health and care
7. ensure that any relevant due diligence checks are carried out where processors or sub-processors are involved
8. document the decision-making process to demonstrate accountability

Each requirement has a set of checkpoints. Every ShCR will need to gain satisfactory assurance on each checkpoint before proceeding with data sharing across the ShCR member organisations. Where a ShCR already has a shared local health and care record in place, they should use the checkpoints to assure themselves. They should also have an independent assurance panel to ensure that they are compliant.

ShCRs must meet the requirements set out in this IG Framework. Other areas, that are delivering integrated care, are not presently mandated to use the framework. They are however encouraged to do so to help adopt good practice and comply with the law.

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

Introduction

Having the right information at the right time, in the hands of health and care professionals, saves lives. Health and care professionals need access to patient and service user records to understand their needs and make the best decisions. To enable this, we need to integrate care records across GPs, hospitals, community services and social care rather than each organisation holding information separately in silos.

During the pandemic, we have seen how critical information sharing is. We need to build upon this ensuring that all those caring for a patient or service user have timely access to relevant information. The Caldicott Principles set out that the duty to share information for individual care is as important as the duty to protect confidentiality. Through this framework, we aim to empower local areas to feel confident that this principle is being implemented so that patients and service users truly benefit from joined up care.

NHS England and Improvement has made it clear that each Integrated Care System (ICS) needs to 'develop or join a shared care record joining data safely across all health and social care settings, both to improve direct care for individual patients and service users, and to underpin population health and effective system management'.

The content of an individual's health and care record will be based on professionally agreed standards developed by the Professional Records Standards Body (PRSB). This is called the Core Information Standard. Professionals across a wide range of different sectors, as well as patients, service users and carers have been involved in the development of this standard. They have suggested what information should be recorded at various points of care, from birth, through life events, maternity and end of life, and how it should be done.

The standard will support front-line health and care professionals to access the pertinent information about an individual. It will enable health and care professionals to:

- view a consolidated medication record
- run algorithms where there may be gaps in care, for example, child overdue for immunisation
- identify individuals at risk
- proactively notify other health and care professionals

This will be underpinned by controls to ensure that information is secure.

1.1 PURPOSE OF THE FRAMEWORK

The invitation to participate in the LHCR (now ShCR) programme promised: 'This will all be undertaken within a consistent national framework of IG which will assist exemplars to meet their legal obligations'.

This document, written in a practical style for IG professionals, provides the promised framework. It will help them to ensure that health and care data is used in an appropriate and transparent manner. It will support ShCRs 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
- professional standards and guidelines on sharing information as set out for health and care staff

The framework will also be helpful for all those who are involved in using health and care information generated by individual ShCRs. It provides advice around some of the complex areas which will be relevant to ShCRs such as joint controllership and considering a patient's or service user's choices about how their data is used. It provides tools and templates for organisations to use (refer to Appendix 7). It will help ShCRs to develop their IG capabilities and build trust with the people they serve.

The framework will be a working document which evolves over time to meet the needs of those who use it. It will be updated as required to take into account operational experience and any changes to policy, technology and the law.

In association with this IG Framework, technical architecture capability documents have been prepared (you will need to sign in). These set out the system functionality to be developed including user authentication, care record access audit, role based access controls and handling individual's preferences.

Using the IG Framework

This IG Framework is structured around "journeys". The current journeys are:

- **Journey 1:** Sharing personal/CPI between health and social care bodies within a ShCR for the individual care of patients or service users.
- **Journey 2:** Sharing personal/CPI between health and social care bodies across geographical boundaries for the individual care of patients or service users.

A set of requirements at the start of the IG Framework covers both journeys. A specific set of requirements is then set out for each journey. In terms of practical use, a ShCR needs to work out how it will use information and where it will flow between the ShCR members. This then becomes the basis for working through the relevant IG requirements which are set out in this Framework.

The requirements are accompanied by assurance checkpoints to assess attainment. An assurance checklist is available at Appendix 3. ShCRs should complete this and submit it to the external IG Assurance Panel as part of the assurance process. The Assurance Panel consists of national IG subject matter experts. ShCRs need to achieve satisfactory assurance on each checkpoint and be fully compliant across all checkpoints for Journeys 1 and 2. In the event that satisfactory assurance cannot be met, the ShCR will need to produce an action plan to discuss with the Assurance Panel.

Many "participating organisations" within the ShCR may already have mature systems, which aid the delivery of IG commitments and requirements. It is anticipated that these local delivery systems will continue, however they must be externally assured. ShCRs must use the assurance checklist to assure themselves and the Assurance Panel that they are compliant with this IG Framework even where they have existing systems in place. Where ShCRs have IG policies or are using systems that do not meet the legal requirements set out in this IG Framework, then these policies or systems must be upgraded to meet the IG Framework requirements. For example, if they are not providing transparency information as required by the UK General Data Protection Regulation (UK GDPR). Where current systems do not meet current good practice (but are legally compliant) we do not expect ShCRs to take immediate action to upgrade systems if this may have disproportionate cost implications. If ShCRs do not have policies or systems that meet IG Framework criteria, then they will need to provide evidence of their plan to upgrade systems as part of the ShCR assurance process.

Finally, the IG Framework includes tools and templates which should reduce unnecessary burden and bureaucracy (refer to Appendix 7).

The IG Framework is developed and overseen by the National ShCR IG Steering Group chaired by NHSX. The ShCR IG leads will be in regular contact with the National ShCR IG 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 IG Framework and to assist in developing tools, templates, models and share good practice.

Requirements

The following requirements help support improved access to data, streamline data sharing pathways and ensure legal accountability obligations are met. They are essential for ShCR in IG compliance and good practice and need to be considered for both journeys.

3.1 THE IMPORTANCE OF GOOD IG PRACTICE FOR SHCRS

The UK GDPR stipulates the requirements for controllers and processors. It also sets out 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 or care professional or be closely supported by such a person.

It is important that health and care professionals are represented in discussions about ShCRs. This is particularly important in relation to processes, for example to ensure that IG decisions do not create an unintended burden. It also ensures that a clinical view is factored into processes such as dealing with Subject Access Requests (SARs) or considering whether to uphold an individual's objection to sharing information.

Each ShCR will need a consistent approach to IG policies, processes and systems to ensure good practice across the ShCR. To achieve this, one individual will need to take the lead for a ShCR's IG approach and work with their IG colleagues within the ShCR's constituent organisations. The ShCR Accountable Officers should decide which IG representative takes the role of IG Lead. They will need to be a subject matter expert and they are likely to be a DPO (although this will not necessarily be the case in every ShCR). The ShCR IG Lead should be a senior post with the power to make sure that IG policies are put in place and followed.

The ShCR IG Lead should implement a communications channel with IG representatives in each of the ShCR organisations. They should represent their colleagues, provide a conduit for communications, and become a member of the ShCR IG Leads Network who meet on a regular basis. As part of the ShCR IG Leads Network, good practice from local systems should be shared and capitalised upon. Representation from this network will be required at the national strategic IG network (SIGN) meetings. The IG Lead will also be required to work with Caldicott Guardians, as well as local IG staff. Organisations must ensure IG resource is planned and budgeted for to meet the requirements set out above for an IG function.

Assurance checkpoint

- Appointment of a ShCR IG Lead (subject matter expert)
- ShCR IG Lead is a member of the ShCR IG Leads network
- Structure chart for ShCR IG function (including a communication strategy)
- Evidence of IG policies

Further guidance, tools and templates

- NHS Digital: Key roles and the DPO guide
- Skills for Care: The role of the Data Protection Officer
- Local Job Descriptions: Appendix 7
- Local IG Meeting Structure: Appendix 7

Information Governance Framework for Integrated Health and Care: Shared Care Records

3.2 DETERMINING DATA FLOWS AND CONTROLLERSHIP

ShCRs must demonstrate compliance with the law by mapping data flows and determining roles and responsibilities. One of the most important challenges in the planning stages is to identify the flows of the data and at each point in the process determine who the controllers and/or processors 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 ShCR. A data flow mapping exercise will also inform your Data Protection Impact Assessment (DPIA), assisting you in accessing data from other organisations such as NHS Digital.

An individual's health and care record will assist health and care professionals by bringing together content from across different venues of care that can be standardised and then displayed consistently. An example is by providing a consolidated medication list. This should provide the health and care professionals involved in an individual's care, with confidence that they are accessing timely, complete, accurate and relevant information for the care episode. However, the framework approach recognises the variance that we currently have in how data is captured and represented in local systems.

Nationally, we have worked closely with ShCR/(LHCR) exemplar localities to learn lessons from existing architectural approaches. Whilst ShCRs are operating to a common architectural model, this is being implemented in different ways. There are differences in how data is captured at the point of care, digital maturity and local coding. There is therefore a 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 a data layer, where data is held within the ShCR, is the most appropriate mechanism to ensure data is available in a standardised format. An alternative option to creating a data layer is retrieval of data on demand from source systems. This option will be explored by the ShCRs and may provide a future model where data remains resident within its host systems and is retrieved on demand.

3.2.1 Joint controllership

The UK GDPR and DPA 18 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 ShCR will work as joint controllers with other members of the ShCR areas.

This is 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 ShCR. As a ShCR is not a legal entity, joint controllers will need to enter into binding contracts or processing agreements with processors as a "grouping" of controllers rather than appoint a single lead controller to act on behalf of the grouping.

Data protection legislation requires joint controllers to be transparent about their respective responsibilities. They must ensure that individuals know whom to contact when wanting to exercise their information rights under the legislation. Information about the joint arrangements must be made available to individuals. Irrespective of the joint arrangement, an individual may exercise their rights in respect of and against each controller. Good processes therefore need to be in place to manage such situations.

Presently the way in which this can be met is by setting out an agreement containing the details of those involved in the joint ShCR controllership and how it will work (a 'joint controller agreement'). A joint controller agreement must be an operating model that documents the legal basis and the roles and responsibilities of each controller in the grouping. It should detail common rules for things such as retention and disposal. The agreement should specifically explain who will deal with requests from individuals to exercise their rights under the UK GDPR. For example, as part of the joint controllership arrangements, the constituent legal entities need to agree how they will handle SARs. This should include 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 (UK GDPR Article 28), nor is it a legal "service level agreement".

It is sensible for ShCR areas to bring together their suite of agreements into one place, regardless of what type of agreement it is. 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, UK GDPR Article 26 (joint controllers) details how joint controller arrangements must be set out and how liabilities and responsibilities for compliance are allocated, managed and if necessary indemnified. Joint controllers can be held "jointly liable" if collectively they are responsible for any breach of data protection law. However, the Information Commissioner's Officer (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) are likely to be liable if there is a failure.

3.2.2 Processors

A processor should only be selected and engaged if the controllers have been provided with sufficient guarantees that appropriate technical and organisational measures have been implemented. The joint controllers should be satisfied that the obligations of data protection law (Articles 28, 29, 30 and 32 of UK GDPR) and the rights of the data subjects are met. Any use of a processor must also be aligned with contractual obligations. Suppliers of software and services to care organisations are required to complete the Data Security and Protection Toolkit (DSPT) (refer to Section 3.6.1).

Processors may only act under written instruction from a controller. Therefore, if using a processor, a written contract must be in place between the group of organisations acting as joint controllers and the processors. 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. The written instruction should set out what elements will be required for example telephone support, which may require access to health and care data.

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 are also required to have a DPO. The ShCR IG Lead should take responsibility for liaising with the DPO in the processing organisation to ensure clarity and compliance.

Processors must gain authorisation from the controllers if they wish to subcontract to a third party. Processors 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. Technical specifications such as role-based access, overrides etc. must be carefully considered and all the controllers comfortable with the arrangements.

All GP Practices will use a clinical system of their choice. This is usually procured by the Clinical Commissioning Group (CCG) on behalf of its member practices. The GP practices will sign an agreement allowing the CCG to procure a system on their behalf. The CCG signs a contract with the supplier of choice to enable them to call off products on behalf of the member practices. As part of this procurement, 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 data sub-processor. It provides assurances to GPs that compliance will be adhered to in relation to data protection law.

3.2.3 Data sharing arrangements

ShCRs will share health and care information with other health and care organisations that are not part of the ShCR. At times this sharing will be done on an ad-hoc basis but in some situations the sharing will be more regular. For example, when an adjacent ShCR area contains specialist treatment centres.

There may also be occasions where a ShCR organisation receives a request for information about a patient or service user from outside the health and care family of organisations. These requests should be considered on a case-by-case, rather than automatically sharing. The DPA18 and the Common Law Duty of Confidentiality (CLDC) requirements must be taken into account. There may also be condition-specific legislation that places particular requirements on the controller (for example, Gender Recognition Act 2004). Where approval is given to share information, you will need to have a Data Sharing Agreement (DSA) in place between the organisations involved.

The ICO's Data Sharing Code of Practice covers how to approach ad-hoc and more regular data sharing and how to record activities using DSAs. In accordance with the Code, a DSA (sometimes called an information sharing agreement) is useful in setting out the purpose of the sharing, which organisations are involved and who is responsible for which elements of data protection compliance. It will also help you to demonstrate compliance with the accountability principle in UK GDPR. NHSX has produced a template DSA that can be used by all NHS and social care organisations. The template provides a high-level summary of the minimum data sharing obligations required between parties to ensure lawful data sharing. The template can be built upon to satisfy local needs. 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. The law sets out that 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. When formal regulatory action is being considered by the ICO then the arrangement made between controllers is irrelevant for these purposes.

Assurance checkpoints

- Joint controller agreement agreed by all members of the grouping
- DSA or protocols, where applicable
- Service level agreements, where applicable
- A processor 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
- A completed and approved DPIA for each data sharing purpose to be published in participating organisations publication scheme (except for security and storage arrangements)

Further guidance, tools and templates

- ICO: How do we document our processing activities?
- NHS Standard Contract: data processing agreement
- NHSX Joint Controllers Issues to Consider: Appendix 6
- Local Joint Controller Agreement: Appendix 7
- Thames Valley & Surrey: Local Data Sharing Protocol
- Thames Valley & Surrey: Local Information Sharing Agreement
- Local Contract for the Provision of IT Services: Appendix 7
- Local Data Protection Contract: Appendix 7
- Local Lead Controller Group: Terms of Reference

3.3 UNDERSTANDING LEGAL REQUIREMENTS

ShCRs must demonstrate compliance with the law by identifying the legal conditions for processing information. It is important that each ShCR identifies and understands its legal basis for processing data for every function carried out under the ShCR grouping.

The legal basis and IG 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 purposes for which the data will be used
- complete a DPIA 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 organisations who wish to process the data
- be clear that the public would not be surprised that that sort of data is to be used for that purpose

Where there is joint working between organisations involved in a ShCR grouping, there is no one legal entity. Each organisation has its own legal responsibilities as a controller and will require its own legal basis for the processing. (For more information refer to the section on joint controllers and Appendix 4).

There are six consistent legal parameters which must be considered when sharing personal/CPI for any purpose:

- Statutory requirements and responsibilities including legal restrictions
- Data Protection Act 2018 (UK GDPR) lawfulness for processing
- CLDC
- Human Rights Act obligations
- Health and Social Care Act 2012
- Health and Social Care (Quality & Safety) Act 2015

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

3.3.1 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. For example:

a. CCGs and NHS England have a duty to commission health services, but this does not confer an automatic power to process personal/CPI for their commissioning purposes.

b. 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.

The Standard Contract (GC21.12) 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 UK GDPR (Public Task - Article 6). However, the conditions of Article 9(3) must also be met where relevant.

3.3.2 Data Protection Act (DPA) 2018 and UK GDPR

The data protection principles are found in the UK GDPR Article 5 and organisations are reminded to ensure they comply with these principles.

The UK GDPR also offers individuals' 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 to ensure the appropriate management of individual rights. For more detail on individual rights and restrictions under UK GDPR refer to Section 3.4 and Appendix 4.

To ensure legal compliance, the requirements of the UK GDPR and the DPA 18 must be met.

Chapter 2 of the DPA 18 is relevant to most processing of personal data therefore it is important that the UK GDPR and DPA 18 are read side by side. Each ShCR must 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 personal data (such as health information) controllers will also need to identify a separate condition for processing as described in UK GDPR Article 9.

In practice, for much of the data processed in health and care there will be a two-stage process. The first stage gives the lawful basis as applied to all personal data (Article 6 of the UK GDPR). The second stage applies because you are processing a special category of personal data, data concerning health (Article 9).

First stage

It is for controllers to determine their lawful basis. The lawful basis for processing must be recorded.

The most appropriate basis for lawful processing that is available to funded and/or statutory health and social care organisations in the delivery of their functions is Article 6(1)(c) or Article 6(1)(e).

Generally, many health and care settings have a lawful basis for processing personal data. This is because it is necessary 'for the performance of a task carried out in the public interest or in the exercise of official authority' (Article 6(1)(e)). 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.

In some circumstances, the controllers could also decide that the processing is necessary for 'compliance with a legal obligation' where they have such an obligation to provide care (Article 6 (1)(c)).

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 Article 6(1)(c). Any service provided beyond the contract will be covered by Article (6(1)(e).

In the case of locally commissioned services Article 6 (1)(b) 'for the performance of a contract' may be considered. 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).

Article 6(1)(d) to protect the vital interests of the data subject may also be appropriate, for example, in the case of an emergency.

Do not use consent as a condition for processing to meet UK GDPR and DPA 18 requirements, unless in exceptional circumstances. Should specific processing arise in which explicit consent is required by law, for example, Human Fertilisation and Embryology Act 2008 and Gender Recognition Act 2004, then please refer to UK GDPR recitals: 32, 42 and 43.

Second stage

Special categories of personal data, including data concerning health, may be processed only for reasons specified in Article 9 of the UK GDPR. In the case of most health and care settings, the reasons are generally for:

- 'the provision of health care or treatment'
- 'the management of health care systems or services or social care systems or services'
- '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 CLDC under a legal provision (as listed in DPA 2018 s204), must be responsible for the processing.

3.3.3 Common Law Duty of Confidentiality (CLDC)

The CLDC will need to be considered when sharing information for ShCR. 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 CLDC means that when someone (such as a patient or service user) shares personal information in confidence (to a healthcare 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. That is unless there is another valid legal basis, such as a court order, statutory gateway which allows confidentiality to be set aside, or overriding public interest. Where a patient or service user has agreed to a programme of treatment and care, it is assumed they have agreed to the use of their relevant information to support that programme of treatment being shared with others who are involved in their care. This is known as implied consent.

In certain situations, other than for individual care reasons, approval may be sought from the Confidentiality Advisory Group (CAG), which is part of the Health Research Authority (HRA). CAG have the power to advise on setting aside the CLDC, usually for research purposes, under Section 251 of the NHS Act 2006.

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', (for example, a health or adult social care commissioner or provider, hence it is a corporate duty, not an employee'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. This accords with the 7th Caldicott principle. However, the obligation 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 to processing can be raised (refer to section 3.5 on objections).

In delivering individual care, it is reasonable and lawful 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 care. Unlike the high threshold for consent (where applicable) under UK GDPR, the same standard of consent is not necessary to satisfy CLDC. Consent under the CLDC may therefore be implied for the sharing of all information relevant to the care of the individual. This is unless an individual specifically objects to CPI being shared

for these purposes. Although implied, individuals with capacity also have the right to withdraw consent for the use of their information, even if this impacts the care that is being provided or is to be provided so long as this has been explained to them. Where health and care information is accessed, only relevant information should be seen as governed by access controls and professional codes of conduct (see Section 3.4).

To use implied consent, organisations must inform patients or service users of how their information may be used when providing services. Transparency is a mandatory requirement under UK GDPR. Organisations need to ensure that patients or service users are as informed as possible. This could be through discussions with health and care professionals, information leaflets, and comprehensive transparency materials (Refer to Section 3.3.5 for more details on transparency).

3.3.4 Meeting the Human Rights Act 1998 obligations

The Human Rights Act (article 8) 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. A public authority abiding by the UK GDPR and the CLDC is likely to meet the Human Rights Act obligations. This is because the UK 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 is proportionate. A DPIA must be completed at an early stage to identify any risks to the processing of personal data. For further information regarding DPIAs, refer to Section 3.7.2.

Assurance checkpoints

- A statement for each organisation involved in the collective sharing setting out the purpose, lawful basis for processing and CLDC satisfied.
- Transparency information stating what data is collected, stored, shared and retained and for how long. The transparency information must also include information on patient or service user preferences, where applicable.
- An agreed approach across the ShCR for the management of patient or service user objections to share their data for individual care.
- Evidence of effective Role Based Access Control (RBAC).
- Evidence of completed and approved DPIA for each data sharing purpose to be published in participating organisations publication scheme (except for security and storage arrangements).

Further guidance, tools and templates

- Department of Health and Social Care: Confidentiality Code of Practice
- General Medical Council: Confidentiality: good practice in handling patient information

3.3.5 The Duty of Transparency

ShCRs must demonstrate compliance with the law by ensuring transparency about purpose and process. A new requirement of the UK GDPR is the principle of *accountability* which requires that organisations must not just comply with the law but be able to demonstrate that compliance.

The duty of transparency is also one of the ways we can build trust and gain the respect of the public in the use of their data. The aim of transparency is to ensure there are 'no surprises' for the patient. This is now enshrined as the eighth Caldicott Principle - Inform patients and service users about how their confidential information is used.

Part of the transparency requirement involves the provision of information to the public via transparency materials – previously referred to as privacy notices. A specific requirement of the UK GDPR is that organisations must include their lawful basis for processing information in their transparency materials. Individuals must also be informed of their right to object to processing and how to exercise that right (refer to Section 3.5). 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 (UK GDPR Articles 13 and 14).

The law gives discretion to controllers to consider where this information 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

There are 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.

Care must be taken if conveying information to children, as more specific obligations will apply. The ICO has guidance on Children and the UK GDPR including how the right to be informed applies.

Online 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) (see Section 3.3.6), data sharing flows etc, can all contribute to this aim (consider publishing under the Freedom of Information Act 2000).

It is helpful, if possible, to involve communications professionals in the transparency process. It is important to ensure that the production of materials, language and channels used are appropriate. To ensure consistency throughout the ShCR, it is important that the same messages and language are used. When new organisations join the ShCR, transparency information will need to be updated. Equally, to ensure consistency across the system, template text for national initiatives such as the Summary Care Record or local requirements such as DPIA and transparency materials should be adopted.

Assurance checkpoints

- Production of a clear plan, list of communication materials and channels
- Transparency materials stating what data is collected, stored, shared and retained for how long). The material should also include information on patient or service user preferences, where applicable
- Publication of information and transparency materials by all participating organisations in the ShCR to the public, patients or service users
- Details of a process for managing and updating communications
- Evidence of public engagement to gain their view of the approach and test materials
- Demonstration of how patients or service users can exercise individual rights in transparency documentation

Further guidance, tools and templates

- Carnegie Trust: Data for public benefit
- Connected Health Cities: About our public engagement
- One London: Public deliberation in the use of health and care data
- Yorkshire and Humber Care Record: Fair Processing Notice
- Local Comms Delivery Plans: Appendix 7
- Thames Valley & Surrey: Ethics and Engagement Advisory Board and Terms of Reference

3.3.6 Records of Processing Activity (ROPA)

UK GDPR Article 30 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 transparency information 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. This should show when, why and how that data is processed for what purposes, with whom it is shared. It should also set out the retention periods.

The registers must 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.

Assurance checkpoints

- Policies and procedures for information asset management
- ROPA/Production of an Information Asset register/ROPA list

Further guidance, tools and templates

- ICO: Documentation of processing activities
- Digital Social Care: How to document your data processing
- Local ROPA: Appendix 7

Organisations that process health and care information must also have an Appropriate Policy Document (APD) set out in Article 30. This must outline:

- the legal basis upon which the processing is taking place
- compliance with UK GDPR Principles (Article 5)
- how long you retain, and/or the erasure of, personal data. If these retention periods are not followed, or personal data isn't to be erased at the end of processing, you must explain why

The APD does not need to be a specific document titled as such. An APD may be a local Records Management Policy, that sets out within it the points mentioned above.

You do not need a separate APD for each processing activity or condition relied upon. You could have a single document that references the processing undertaking in its various forms and cite which policy or guidance document can provide the necessary detail.

The APD is not designed to be a standalone document detailing every processing activity you undertake. It is aimed at complementing your general ROPA commitments, giving further protections and accountability to the personal data you are processing.

APDs must be seen as an iterative document. They must be retained for at least six months from the end of the processing activity to which they relate. When a service changes operationally, the relevant guides and documents for that service must also be updated to reflect the new changes and still cover the bullet points listed above.

The ICO may ask to see your APDs. If so, you must give it to them free of charge and as soon as reasonably possible following the request. Further guidance can be found on the ICO's website.

3.4 DATA ACCESS CONTROLS, SUBJECT ACCESS REQUESTS, REVIEW AND RETENTION

ShCRs must ensure compliance with the law by promoting the application of appropriate technical and organisation measures. When accessing data for individual care purposes, consideration must be given to the policies and processes used to support that disclosure.

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. ShCRs need to ensure that only health and care professionals and non-clinical staff who have a legitimate relationship with the patient or service user, providing or supporting their care, will have access to their record.

An appropriate access control model delivers this commitment. A national policy is being developed for this purpose through engagement with national stakeholders and clinical groups. This will set out basic requirements for an access control model as a minimum standard for intra-ShCR data sharing (Journey 1) and cross ShCR data sharing (Journey 2). This will ensure health and care professionals access only relevant and proportionate information from the health and care records of individuals with whom they have a legitimate relationship. The ShCR approach will also provide a feedback loop back to source systems to support the improvement of data quality at source.

Care should be taken to ensure that the ShCR is clear on which individual rights apply and have processes in place to ensure an individual can enact those rights (see Section 3.3.2). The application of individual rights is dependent upon the conditions for processing used for the sharing of the data.

Patients and service users have the right to know certain information about the processing of their personal data by health and care organisations. These include:

- the purpose for processing
- what information is being processed
- who is processing their information
- if they have the right to rectification or erasure of their data
- the right to complain to the ICO
- where information about them is collected from (if not themselves)

This list is not exhaustive, and this information will usually be included in the organisation's transparency materials created for patients or service users.

ShCRs must include high-level audit functionality which enables controllers to meet their access control responsibilities. It should also provide information to individuals about which organisations have accessed their records, when and why. Some audit trail functionality may enable individuals to also see what activity was done in the record. Patient or service users have the right to challenge that access.

There needs to be a process in place to ensure that SARs to the ShCR are responded to. This must be detailed in the joint controller arrangement. 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

An example of a process which has worked well in some areas is an information sharing group, which is established to lead on the request handling. In the event of a SAR, each organisation contributing to the ShCR 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. In such cases the 'holding' organisation should deal with the request on an exclusive basis. One option to do this could be that organisations may respond by facilitating online access by the individual to their own record. However, where this is not possible, the organisation can provide a 'sealed' redacted record (either on paper, CD or other media) to the 'holding' organisation to pass to the individual.

Organisations must avoid a situation where a management fee can be charged by the co-ordinating body. 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.

It is also important to note that the CLDC applies to deceased patients and any third parties identified in the record. If there are requests to access the deceased's patient information, then these need to be considered under the Access to Health Records Act 1990.

Where data is held within the ShCR, then each ShCRs must ensure that they retain records in an accessible format until the relevant retention period is reached. This is in line with the Records Management Code of Practice 2021. 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 or deleted

Assurance checkpoint

- Compliance with the Records Management Code of Practice for Health and Social Care 2021
- Audit of IG policies
- Effective Role Based Access Control (RBAC)
- Process in place for complying with individual rights where required, such as rectification, objection and SARs

Further guidance, tools and templates

- NHS Digital: Registration Authorities and Smart Cards
- Local Information Sharing Agreement - includes section on RBAC Roles and Objections, Appendix 7

3.5 PATIENT AND SERVICE USER OBJECTIONS TO PROCESSING

3.5.1 Common law duty of confidentiality

There are two legal considerations here; the duty of confidentiality and data protection law. In most circumstances the former will be relevant when proposing to share information for the purposes of providing individual care while the latter is broader and could include individuals objecting to the retention of certain data.

Although consent for delivering individual care is implied, individuals with capacity also have the right to withdraw consent for the use of their information. This is the case even if it impacts the care that is being provided (or is to be provided) so long as this has been explained to them and in particular the consequences of the withdrawal. For example, if an individual states that they do not wish to share a specific piece of information as part of the ShCR, then you should respect their wishes. The individual does not need to justify their reasons unlike the right to object under UK GDPR as set out below.

3.5.2 UK GDPR

UK GDPR gives individuals the right to object to the processing of their personal data and have their objection considered (Article 21). The right to object is particularly relevant to certain health and care organisations where lawful processing is based on a 'task in the public interest' provision. If someone objects to you processing their 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'.

All ShCRs must ensure procedures are in place in relation to individuals' objections under UK GDPR as a minimum. Organisations need to ensure that where objections have been received, procedures and processes are in place to consider and respond. While it is unlikely that an objection would be upheld where it concerns a health and care record, objections must be considered on a case-by-case basis. This allows IG professionals to work with their clinical colleagues and Caldicott Guardian to make the decision to uphold or reject the request. An individual should give specific reasons why they are objecting to the processing (which covers any use of the data including the recording of it and sharing it) of their data based on their particular situation. Individuals 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. This will differ from case to case. Controllers will then need to consider whether their own requirements override that of the individual.

Although UK GDPR does not give a specific definition of compelling legitimate grounds, there is guidance from the ICO on legitimate interests. 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. It includes information about Legitimate Interest Assessments (LIA) which involve a three part test. Controllers are encouraged to ask the right questions about processing and objectively consider the reasonable expectations of the individual, together with any impact of the processing on them. The Balancing Test (part 3 of the LIA) covers the need to consider the interests and fundamental rights and freedoms of the individual.

3.5.3 Local policies in relation to choices

Some ShCR areas have provided mechanisms for patients and service users to state a preference over whether they have a shared record, for example, by providing an opt-out form. Again, this is a local policy decision. It is important however, that this local mechanism for stating a preference is not confused with the right to object under UK GDPR where each objection needs to be considered and responded to on a case-by-case basis. Communications with patients or service users should be clear and distinguish between the right to object under UK GDPR and an individual's preference around data sharing.

Some ShCRs may go beyond this following local discussions with health and care professionals, patients and service users and implement a local policy where a patient or service user is asked before their record is viewed. This should not be referred to as 'patient consent' but rather "permission to view". Permission to view can help ensure there are no surprises for the patient or service user particularly when a particular role is accessing relevant but more detailed information (see Section 3.4).

Assurance checkpoint

- An agreed approach across the ShCR for the management of patient or service user objections to share their data for individual care

3.6 ASSURING SECURITY

All organisations, including those within a ShCR, are expected to comply with relevant cyber security legislation, policies and guidance. This includes the National Data Guardian's ten data security standards. This will help ensure that people, processes and technology are maintained to ensure cyber security and protect the confidentiality, integrity and availability of records.

It is also important that policies for areas such as staff training, internal audits and HR, and retention and disposal schedules are adhered to. They should be available under FOI requirements, but withholding anything that may compromise the security and integrity of the record.

3.6.1 The Data Security and Protection Toolkit (DSPT)

The Data Security and Protection Toolkit (DSPT) is a compliance framework that covers all aspects of security and confidentiality. Its focus is on building trust in health and care IT systems. All organisations processing patient and service user data must meet the DSPT requirements.

The DSPT is based on the National Data Guardian's ten data security standards. It is linked with, and supported by, the National Cyber Security Centre, the agency tasked with protecting critical infrastructure. To meet the relevant standards, including IG standards, all Toolkit questions must be appropriately answered. Organisations must not, however, 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 5 for more information on Data Breach Management.

Assurance checkpoint

- A ShCR Cyber Assurance Framework is in place
- A communications route between the ShCR Cyber Security Lead and the ShCR IG Lead and other Cyber Leads within the ShCR participating organisations

Further guidance, tools and templates

- NHS Digital: cyber and data security
- National Cyber Security Centre

3.7 DEMONSTRATING ACCOUNTABILITY

Accountability is one of the key principles in data protection law and all controllers must be able to demonstrate their compliance (Article 5(2)). The ICO has set out how organisations can demonstrate their compliance. It is therefore imperative that all decision making is documented including who was involved and the rationale or justification behind the decision.

3.7.1 Adopting principles by design and default

All ShCRs must ensure the use of data protection by 'design and default'. Adopting the principles of data protection by design and data protection by default is an important concept for any project or new model of care. It is important that when considering new ways of working, the impact to privacy and confidentiality are factored in at the design stage. That way IG 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. IG should be identified as part of any Project Initiation Documents and should be treated in the same way as finance with the essential criteria, key issues and resources assessed.

ShCRs must comply with the law by minimising the use of identifiable data. To meet the data protection principles when using personal data, the amount of data should be adequate, relevant, and not excessive for the purpose. 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 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 (CSOs) as well as Caldicott Guardians and DPOs should be involved with such decision making.

Further information about the responsibilities of a Clinical Safety Officer is set out in the clinical safety standards. These standards are mandatory under the Health and Social Care Act 2012. Ultimately, this helps health and care staff to provide better and safer care.

3.7.2 Data Protection Impact Assessments (DPIA)

If personal data is to be used, UK GDPR (recital 84) states that 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'. In practice this means a ShCR area must carry out a DPIA. The DPIA needs to be approved by the ShCR DPO or joint ShCR DPOs before any processing of personal/CPI commences. 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.

Assurance checkpoints

- Completed and approved DPIA for each data sharing purpose to be published in participating organisations publication scheme (except for security and storage arrangements)
- IG considerations in Project Initiation Documentation
- DPIA risks incorporated into (organisational/ShCR) risk register including mitigation and management
- Unmitigated high risks are escalated to the DPO and the ICO is consulted
- Consultation with the public on data sharing for integrated care

Further guidance, tools and templates

- ICO: Guidance on data protection impact assessments (DPIA)
- ICO: Sample DPIA template
- Thames Valley & Surrey: Local DPIAs

Journey 1

Sharing personal/confidential patient information (CPI) between health and social care bodies within a ShCR for the individual care of patients or service users.

For individual care purposes, service providers can receive and share special category personal data or CPI 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 for individual care set out in Appendix 1, it will not be considered as individual care and therefore the way in which the IG rules apply will change.

This example tasklist will enable ShCRs to consider their data protection requirements prior to undertaking the processing of personal data. It will help to comply with privacy by design and default. It will also help you to evidence your compliance with UK GDPR Article 30 requirements for ROPA.

Example Tasklist (not exhaustive)

Task	Complete
Understand what data you require	
Identify the lawful basis for your data sharing activities and allocate them	
Describe your care system's structure	
Define how your care system will govern data use	
Demonstrate how you will protect the data	
Ensure appropriate contracts and agreements are in place	
Assure your population that processing is fair and transparent	

Journey 2

Sharing personal/confidential patient information (CPI) between health and social care bodies across geographical boundaries for the individual care of patients or service users.

This journey covers individual care across geographical ShCR boundaries. Where relationships are required or already exist with neighbouring ShCRs such as shared clinics etc, then DSAs should be developed or already in place. For existing DSAs these will need to be reviewed against the NHSX joint DSA.

There may also be circumstances for ad hoc information sharing. In such circumstances, professional judgement needs to be exercised. There must also be 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 provides information for such circumstances.

It is important that information is available at the point of care for a patient or service user. ShCRs need to have in place, an effective access control model which:

(i) allows proportionate access to appropriate and relevant data held within an individual's health and care record by the health and care professional(s) and **only** if there is a legitimate relationship between the professional and the individual

(ii) creates robust audit on each access which can be investigated and challenged, if deemed inappropriate

Where a person receives care at a venue outside of their home ShCR, there is a need to discover where data is held so the data can be retrieved. The requesting organisation will be responsible for ensuring the request is valid.

The intent is for the following capabilities to support the discovery of the location of data for Journey 2:

- Personal Demographics Service (PDS) - provides an API that will return the patient's demographic information and may, in future, return a pointer to their main record
- National Record Locator Service (NRLS) – enables authorised users to find specific patient records that are held on different health care systems

- ShCR Application Programming Interfaces (APIs) – to enable retrieval of data included in health and care records subject to authentication and authorisation

This example tasklist will enable ShCRs to consider their data protection requirements prior to undertaking the processing of personal data. It will help to comply with privacy by design and default. It will also help you to evidence your compliance with UK GDPR Article 30 requirements for ROPA.

Example Tasklist (not exhaustive)

Task	Complete
Understand what data you require	
Identify the lawful basis for your data sharing activities and allocate them	
Describe your care system's structure	
Define how your care system will govern data use	
Demonstrate how you will protect the data	
Ensure appropriate contracts and agreements are in place	
Assure your population that processing is fair and transparent	

Assurance checkpoints (Journey 2 only)

- Completed and signed off Information Sharing Agreements between neighbouring ShCRs
- Cross-ShCR Information Sharing materials that are available to patients or service users at the Point of Care
- Effective Role Based Access Controls (RBAC)

Further guidance, tools and templates

- Yorkshire and Humber Joined Up - insight research
- Yorkshire and Humber Digital Health and Wellbeing Charter

Appendices

APPENDIX 1: GLOSSARY

TERM	DEFINITION
Accountability	Accountability is one of the data protection principles - it makes the controller responsible for complying with the UK GDPR and able to demonstrate compliance.
Application Programming Interfaces (APIs)	This is the way one software application talks to another through what can be thought of as easy to read templates.
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 fingerprint data.
Breach	Any failure to meet the requirements of the Data Protection Act and/or UK GDPR, an unlawful disclosure of CPI 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 health and care professionals, which are responsible for commissioning most health and care services for patients.
Clinical Safety Officers (CSOs)	Appointed to oversee the clinical risk assessment of a health IT product. They should be a clinician with a current professional registration.
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.
Common law	Laws that are based on court or tribunal decisions which govern future decisions on similar cases.

TERM	DEFINITION
Common Law Duty of Confidentiality (CLDC)	This arises when one person discloses information to another (for example, 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; 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 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.
Confidential Patient Information (CPI) or patient information	Defined in Section 251 (10) of the National Health Service Act 2006, patient information means: (a) information (however recorded) which relates to the physical or mental health or condition of an individual, to the diagnosis of his condition or to his care or treatment, and (b) information (however recorded) which is to any extent derived, directly or indirectly, from such information, whether or not the identity of the individual in question is ascertainable from the information. Section 251 (11) states: - For the purposes of this section, patient information is "CPI" where— (a) the identity of the individual in question is ascertainable— (i) from that information, or (ii) from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information, and (b) that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual.

TERM	DEFINITION
Consent	Consent can be used for a number of different purposes, offering individuals real choice and control. When using consent, organisations need to be clear on why they are getting consent (for example to satisfy confidentiality, medico-legal reasons, or for processing data). Explicit consent requires a positive opt-in and must be evidential. The UK GDPR sets a high standard for consent. Often consent is not the appropriate UK GDPR legal basis for processing health and care data, and another lawful basis can be found. However, consent may still be required to meet the CLDC.
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 (DPA) 2018	The DPA 2018 is the UK's implementation of the General Data Protection Regulation (UK GDPR). It transposes the Law enforcement directive into UK law.
Data Protection Impact Assessment (DPIA)	A DPIA is a process to help identify and minimise the data protection risks of a project. Under UK GDPR, 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 (DSA)	A DSA 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 DSA in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

TERM	DEFINITION
Data subject	An identified or identifiable natural person.
Duty of transparency	The UK 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 UK 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 unmistakable. It can be given in writing or verbally, or conveyed through another form of communication such as signing. Whilst explicit consent is not required for direct care purposes, it may still be required to comply with other statutory requirements (such as the Gender Recognition Act 2004).
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.

TERM	DEFINITION
Implied consent	Only applies in the context of care provided to individuals (or actions that lead to the provision of care). Implied consent refers to instances where the consent of the individual patient can be implied, without them having to make any positive indication of their wishes, such as giving their verbal agreement for a specific aspect of sharing information to proceed. An example of implied consent would be doctors and nurses sharing CPI 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. To use implied consent, organisations must inform patients or service users of how their information may be used when providing services. Typically, this could be included in patient or service user information leaflets about a service, or as transparency information on their website about how the organisation uses personal and health and care data.
Individual care	Has the same meaning as *Direct Care. Both definitions below are taken from "Information: To Share or not to Share? The IG Review 2013".* 1. *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.* 2. *Direct 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.*

TERM	DEFINITION
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, IG 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 or joint 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 UK 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 UK GDPR.
Lawful basis	The principle of accountability requires you to be able to demonstrate that you are complying with the UK 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)	A LHCR is a grouping of health and care organisations within a geographical boundary. Now referred to as ShCRs.

TERM	DEFINITION
National Data Guardian (NDG)	The NDG advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly.
Natural person	A living human being with certain rights and responsibilities under law.
NHS Digital Data Security and Protection toolkit (DSPT)	The DSPT replaces the NHS IG 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.
Participating organisation	Participating organisations are those statutory organisations or other legal entities signed up to a ShCR DSA or other organisations contracted by a statutory organisation, which could be a private sector or 3rd sector organisation.
Permission to view	This is where you ask the patient or service user before viewing the record. This can be overridden in certain circumstances, for example, in an emergency where the patient is unconscious.
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.
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.

TERM	DEFINITION
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.
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 UK 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	DPIAs 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 controls (RBAC)	Access to data is dependent on the role of the person, for instance, a receptionist would see different information to a consultant.
Service level agreement (SLA)	An agreement negotiated between two parties where one is the customer and the other the service provider. The SLA records a common understanding about services, priorities, responsibilities, guarantees and warranties. SLAs 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.
Shared Care Record (ShCR) Exemplar	A ShCR is a grouping of health and care organisations within a geographical boundary.
Special category data	Personal data which the UK GDPR says is more sensitive, and so needs more protection. Such data includes health, genetic and 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 UK GDPR Individuals have a right of access to their personal data. This is commonly referred to as a SAR.

TERM	DEFINITION
Third party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor (if they process personal data in their own right then they will also become a controller).
Threat	Any circumstance or event with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data and/or denial of service.
Transparency 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 or as soon as practically possible after the collection. This used to be called a privacy notice.
UK General Data Protection Regulation (UK GDPR)	The EU regulation that was passed in May 2016 and transferred into UK law with the UK leaving the EU in January 2021. It forms part of the new data protection regime in the UK, alongside the Data Protection Act 2018.
Vital interests	Necessary to protect an interest which is essential for the life of the data subject or that of another natural person.

APPENDIX 2: JOINT CONTROLLERS

Joint controllership: what it means

Joint controllers (UK GDPR article 26) decide the purposes and means of processing together – they have the same or shared purposes. Controllers will not be joint controllers if they are processing the same data for different purposes.

ShCRs will be joint controllers, as between them, the organisations involved in the ShCR will be processing personal data for medical and related care purposes. Member organisations of a ShCR will decide on the precise purpose and manner for which personal data is processed within the ShCR.

As a ShCR is not a legal entity, joint controllers will need to set up and record their joint controllership arrangement. Such an arrangement must be clear about how individuals can exercise their data protection rights as well as setting out how the UK GDPR transparency requirements (set out under Article 13 and Article 14) will be met. Members of the ShCR also need to decide on how they will handle any organisations contracted as processors. They should also use the joint controllership arrangement to set out how members will share information within the ShCR to support the delivery of health and care.

How ShCRs can share information between member organisations

'Enhanced sharing': no new external record, rather just a method which allows individual controllers to get a record from wherever it is held within the ShCR membership.

'Combined record': each member organisation contributing to a (probably new) shared record they all have access to.

Whilst being a relatively basic tool the ICO online checklist does provide some points to consider when determining if you are acting 'jointly'.

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 working together and processing the personal data for the same purpose or purposes as another controller.

- We are using the same set of personal data (for example, 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 is a controller to controller arrangement, there is no single overarching shared record. From the ICO checklist this will mean:

- common objective: linked up care, correct information and not having to ask the patient or service user every time
- same set of personal data
- designed this process with another controller – all ShCRs 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 ShCR (DSP toolkit, DP laws, ShCR framework agreement, common training requirements)

Combined model: this isn't controller-to-controller as a joint record is created that requires a common way of working between ShCR members, but similar factors are involved:

- common objective: linked up care records, correct information and not having to ask patient or service user 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 ShCRs work together to establish the system?
- although different organisations policies can still be used within a wider framework as most organisations will want to assure the compliance of others in ShCR (DSP toolkit, DP laws, ShCR framework)

DPIAs and joint controllership

- As joint controllers in a ShCR, it is important that all organisations come together to produce a DPIA covering the ShCR's processing of personal data and implications for members of the ShCR.
- As part of the UK GDPR's transparency requirements, ShCRs should publish their DPIAs on the websites of member organisations. However, the security and storage arrangements used by the ShCR (as detailed in the DPIA) must not be published because the risk of this information being misused.

APPENDIX 3: ASSURANCE CHECKLIST (FOR COMPLETION BY THE ShCRs)

The assurance checklist is intended to provide assurance to ShCRs that they are following the guidance outlined in the Framework. ShCRs should complete a self-assessment by reading each assurance checkpoint and then ticking if they feel there is satisfactory evidence. After the self-assessment is complete and the ShCR feels 'ready', it can make a submission to the IG Assurance Panel. The papers will include a signed off copy of the Assurance Checklist and the supporting evidence detailed within the checklist.

Assurance Checkpoint	Relevant section of IG framework	Evidence Yes or No	ShCR comments
Appointment of a ShCR IG Lead (subject matter expert)	3.1 The Importance of Good IG Practice for ShCRs		
ShCR IG Lead is a member of the ShCR IG Leads Network	3.1 The Importance of Good IG Practice for ShCRs		
Structure chart for ShCR IG function (including communication strategy)	3.1 The Importance of Good IG Practice for ShCRs		
Evidence of IG policies	3.1 The Importance of Good IG Practice for ShCRs		
Joint controller agreement agreed by all members of the grouping	3.2 Determining data flows and controllership		
DSA or Protocols (where applicable)	3.2 Determining data flows and controllership 5. Journey 2		
Service Level Agreement (where applicable)	3.2 Determining data flows and controllership		

Assurance Checkpoint	Relevant section of IG framework	Evidence Yes or No	ShCR comments
A processor contract between the grouping and the processor(s)	3.2 Determining data flows and controllership		
A clear data processing map showing purpose and controller and processor at each stage of the data flow	3.2 Determining data flows and controllership		
Completed and approved DPIA for each data sharing purpose to be published in participating organisations publication scheme (except for security and storage arrangements)	3.2 Determining data flows and controllership 3.3 Understanding Legal Requirements 3.7 Demonstrating accountability		
A statement for each organisation involved in the collective sharing setting out the purpose, lawful basis for processing and, CLDC satisfied	3.3 Understanding Legal Requirements		
Transparency information stating what data is collected, stored, shared and retained and for how long. The transparency Information should include information on patient or service user preferences, where applicable	3.3 Understanding Legal Requirements 3.3.5 The Duty of Transparency		
An agreed approach across the ShCR for the management of patient or service user objections to share their data for individual care	3.3 Understanding Legal Requirements 3.5 Patient and Service User Objections to processing		

Assurance Checkpoint	Relevant section of IG framework	Evidence Yes or No	ShCR comments
Evidence of effective Role Based Access Control (RBAC)	3.3 Understanding Legal Requirements 3.4 Data access controls, SARs, review and retention 5. Journey 2		
Production of a clear plan, list of communication materials and channels	3.3.5 The Duty of Transparency		
Publication of information and transparency materials by all participating organisations in the ShCR to the public, patients or service users	3.3.5 The Duty of Transparency		
Details of a process for managing and updating communications	3.3.5 The Duty of Transparency		
Evidence of public engagement to gain their view of the approach and test materials	3.3.5 The Duty of Transparency		
Patients or service users can exercise individual rights in transparency documentation	3.3.5 The Duty of Transparency		
Policies and procedures for information asset management	3.3.6 ROPA		
Records of Processing Activity, Production of an Information Asset register, ROPA List	3.3.6 ROPA		

Assurance Checkpoint	Relevant section of IG framework	Evidence Yes or No	ShCR comments
Compliance with Records Management Code of Practice for Health and Social Care 2021	3.4 Data access controls, SARs, review and retention		
Audit of IG policies	3.4 Data access controls, SARs, review and retention		
A process in place for complying with individual rights where required, for example, rectification, objection, SAR	3.4 Data access controls, SARs, review and retention		
A ShCR cyber assurance framework is in place	3.6 Assuring Security		
A communications route between the ShCR Cyber Security Lead and ShCR IG Lead and; other cyber leads within ShCR participating organisations	3.6 Assuring Security		
IG considerations in Project Initiation Documentation	3.7 Demonstrating accountability		
DPIA risks incorporated into (organisation/ShCR) risk register including mitigation and management	3.7 Demonstrating accountability		
Unmitigated high risks from a DPIA are escalated to the DPO and the ICO is consulted	3.7 Demonstrating accountability		
Consultation with the public on data sharing for integrated care	3.7 Demonstrating accountability		
Cross-ShCR information sharing materials that are available to the patient or service user at the point of care	5. Journey 2		

APPENDIX 4: INDIVIDUAL RIGHTS

The following provides further information about individual rights in UK GDPR.

1. The right to be informed

The right to be informed covers some of the key transparency requirements of the UK 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).

2. The right of access

Individuals have the right to access their personal data which is commonly referred to as a *Subject Access Request* (SAR). 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. The ICO has produced a Code of Practice for SARs. Further information on SARs is also available on the NHSX IG portal which includes a set of FAQs.

3. 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 UK GDPR [Article (5) (1) (d)]. The following relevant statements from the NHS Constitution (2013, 2015) and how this right may be applied should also be noted:

"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" (page 56) The Handbook to the NHS Constitution 2013.

The NHSX Template Data Sharing Agreement: Short Guide for Users, defines a process that can be adopted for communicating rectifications of personal and special category information between organisations.

4. The right to erasure

Individuals have a right to have certain personal data erased, commonly known as "the right to be forgotten." The right to erasure only applies where data is processed under consent.

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 explains 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." Health and care professionals may advise patients or service users that certain data cannot be removed because it allows continuity of care for their wellbeing.

Relevant exemptions to this right include:

- if the data collection took place to comply with legal obligations
- the exercise of official authority
- in the public interest relating to public health

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

5. 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).

6. 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.

The right to portability applies if the data processing is automated and the legal justification is consent. Where the organisation's lawful basis is public interest (task), the rights of portability do not apply.

7. 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.

8. Rights in relation to automated decision making and profiling

The UK 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 UK 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 UK GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision.

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 5: 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.

UK GDPR introduces a duty on all organisations to investigate security incidents to establish whether a personal data breach has occurred. Therefore, a robust breach detection, investigation and internal reporting procedures need to be in place.

If a personal data breach has occurred, organisations need to promptly take steps to address this. This includes 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.

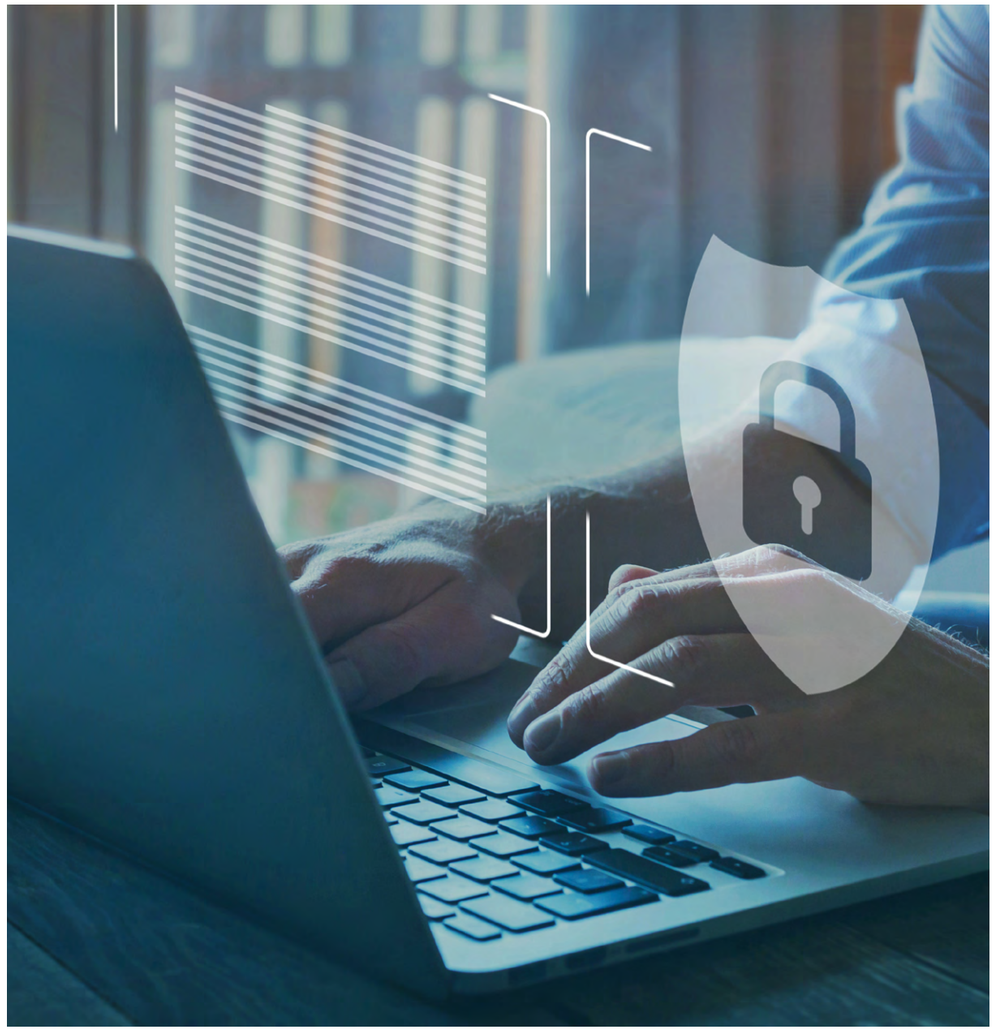
Any breaches that also fulfil the criteria of a "Security of Network and Information Systems" (NIS), a notifiable incident will be forwarded to the DHSC. The Secretary of State is the competent authority for the implementation of the NIS directive in the health and social care sector. The ICO remains the national regulatory authority for the NIS directive.

Useful documents and guidance

The NHS Digital Data Security Standard 6: Guide to the Notification of Data Security and Protection Incidents 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. This includes organisations registered with the Care Quality Commission (CQC). It also includes organisations processing health and social care personal data under contract with the health and social care sector. This includes directly commissioned services and their support services.

For health and care organisations (or those organisations processing health and social care data under contract), breaches are reported using the Reporting Tool within the DSPT. 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 or report to the ICO directly. The ICO has produced some useful guides on their website which sets out a data breach management and reporting process.



APPENDIX 6: JOINT CONTROLLERS: ISSUES TO CONSIDER

Introduction

This guidance outlines the main issues that you need to consider when acting as a joint controller and it should support you when signing up to a joint agreement. It should help, in particular, when you are one of a large number of joint controllers for example if you are working with a large number of organisations to provide integrated care.

For more detailed guidance, the ICO has published a statutory Code of Practice on Data Sharing, which covers all aspects of this area.

What is a joint controller?

The Data Protection Act 2018 provides a definition of a controller.
There are two types:

- sole controller
- joint controller

A sole controller is an organisation that decides, by itself, the purpose for, and the manner in which, personal data is to be processed. For example, a GP practice may make a decision to run an exercise to find out which of their patients are most at risk of hospital admission or developing a particular condition.

Joint controllers are organisations which, between them, decide on the purpose and manner for the processing and have the same or shared purposes. Controllers will not be joint controllers if they are processing the same data for different purposes.

To be joint controllers, there must be more than one organisation involved, the number can be unlimited. A GP practice would be a joint controller, for example, if it was contributing information to a shared record and where all organisations were using that information to make decisions to provide care.

Signing up to a joint controller agreement

As a joint controller you will need to be clear about:

- your role and responsibilities; and
- the role and responsibilities of the other controllers you are entering into an agreement with.

This can be achieved through an agreement containing the details of those involved in the joint controllership and how it will work. This is called a joint controller agreement.

The following sets out areas to consider when signing up to a joint controller agreement for a Shared Care Record Programme (ShCR).

Issue to Consider	Questions	Yes or No	Further Information
Risks and mitigations	Has a DPIA been completed for the ShCR and are you happy that the risks have been appropriately identified and mitigated?	Y or N	A DPIA is a process to help identify and minimise the data protection risks of a project. This is required for processing that is likely to result in a high risk to individuals. The DPIA must be completed before you sign the agreement.
Purpose	Are you clear for what purpose the data is being shared?	Y or N	It is important that the agreement is clear about the purpose for processing. This also supports transparency with the public. If the purpose changes the agreement must be updated and information must be displayed to inform patients of this change.

Issue to Consider	Questions	Yes or No	Further Information
Legal Basis for processing data	Are you clear about the legal basis for processing the data?	Y or N	The agreement must clearly document the legal basis for processing the data. This should include 3 parts: • **UK GDPR -** the legal conditions for processing personal and special category data under UK GDPR (a condition from Article 6 and 9) • **Common Law Duty of Confidentiality** - for individual care, it is reasonable to rely upon implied consent. For other purposes the agreement will need to be clear how the common law is being met (for example, by seeking explicit consent) or set aside (for example, through section 251 support). • **Statutory powers-** If you are a public body, does the processing match your statutory functions. GPs will not have statutory powers, but derive their powers and abilities based on their service provision contract (GMS/PMS contract).

Issue to Consider	Questions	Yes or No	Further Information
Roles and Responsibilities	Are you clear about which organisations or individuals information will be shared with or accessible by. For example, trusts, care homes etc? Has the ShCR identified any processing which requires the use of a processor?	Y or N	The agreement should clearly set out which other joint controllers are signing up to the agreement. There should be a separate contract if a processor is used. This should not be part of the joint controller agreement but requires a separate written, legally binding contract in place between the ShCR IG lead and the processor. It is important that you understand these arrangements prior to signing a joint agreement. For example, the ShCR IG lead should provide evidence that they have conducted due diligence on the processor to ensure legal and regulatory compliance.
Retention of Records	Are you clear about how long records will be retained?	Y or N	The agreement should set out how long records will be retained. In addition the ShCR should have a policy or guide that states how long records will be kept for and what will happen once the retention period has expired (known as the Retention and Disposal Schedule)? The retention period should be in line with the Records Management Code of Practice.

Issue to Consider	Questions	Yes or No	Further Information
Relevance of data	Does the agreement clearly set out what data is being processed?	Y or N	This includes the data to be shared, for example, diagnosis and whether the data is identifiable or not. In relation to the data to be shared the PRSB has developed the Core Information Standard through engagement with health and care professionals, patients and service users which defines the content of an individual's health and care record. The ShCR should only use confidential patient information when necessary, for example, data should be anonymised whenever possible and where confidential patient information is required only the minimum amount for the purpose should be processed.

Issue to Consider	Questions	Yes or No	Further Information
Informing the public how their information is used	Is there consistent information for the public on the proposed use of their information?	Y or N	You should ensure that arrangements are in place for informing patients or service users about shared records prior to signing the agreement. The aim of transparency is to ensure there are 'no surprises' for the patient. Part of the transparency requirement involves the provision of information to the public – previously referred to as fair processing. Your local area should have provided information for the public, patients or service users to all joint controllers and you should make sure you display this. This should include accessible information (for example, different languages or formats). Staff in your organisation should know how to signpost patients or service users to further information. You should ensure that arrangements are in place for patients or service users to be informed prior to signing the agreement. There should also be a clear ShCR policy in relation to how complaints will be handled.

Issue to Consider	Questions	Yes or No	Further Information
Records of Processing Activities (ROPA)	Have you got an up to date record of processing which includes information about the ShCR?	Y or N	Before signing the agreement, you should ensure your ROPA is up to date. It should set out: • when, why and how that data is processed • what purposes the data is used for and; • with whom it is shared and retention periods. This can be requested by the ICO at any time. Records of Processing Activity can be linked to privacy notices for ease of transparency.
Patient or Service Users' Rights - Subject Access Requests (SARs)	Does the agreement set out how SARs will be dealt with by the joint controllers?	Y or N	You should ensure that the ShCR has clearly documented policies and processes for handling SARs between the joint controllers. You should make sure you can locate all the information you hold related to a patient or service user and know where to send this information in the event of an SAR relating to the ShCR within the legal time limit (one calendar month from receipt).
Patient or Service Users' Rights - Right to Object	Are you clear about how to handle patient objections?	Y or N	It is important before signing an agreement that you understand how patient or service users objections will be handled. These should be considered on a case by case basis. If you override an objection you should be able to demonstrate how and why your processing of data for individual care provides compelling grounds to override an individual's right to object.
Training	Are staff in your organisation trained?	Y or N	The minimum requirements for staff IG training are set out in NHS Digital's Data Security and Protection toolkit.

APPENDIX 7 – OTHER TOOLS AND TEMPLATES

The following tools, templates and models are available by emailing datapolicyhub@nhsx.nhs.uk. Please specify which number document you require. Many of these documents have been kindly shared by local organisations that are delivering ShCR so that they can be used by others as a template.

1. Data Protection Officer: Job Description Template
2. Head of Information Governance Job Description: Greater Manchester
3. IG Meeting Structure: Greater Manchester
4. IG role descriptions: OneLondon
5. Joint Controller Agreement: South Central West CSU
6. IT Services Agreement: Yorkshire and Humber
7. Data Protection Contract: Yorkshire and Humber
8. Records of Processing Activity: Greater Manchester
9. Communications Toolkit Delivery Plan: Thames Valley Surrey
10. Communications Timeline: Dementia and Frailty Use Cases - Greater Manchester